Robots and Privacy

M. Ryan Calo

Introduction

Robots are commonplace today in factories and on battlefields. The consumer market for robots is rapidly catching up. A worldwide survey of robots by the United Nations in 2006 revealed 3.8 million in operation, 2.9 million of which were for personal or service use. By 2007, there were 4.1 million robots working just in people's homes [Singer 2009, 7-8; Sharkey 2008, 3]. Microsoft founder Bill Gates has gone so far as to argue in an opinion piece that we are at the point now with personal robots that we were in the 1970s with personal computers, of which there are now many billions [Gates 2007]. As these sophisticated machines become more prevalent—as robots leave the factory floor and battlefield and enter the public and private sphere in meaningful numbers—society will shift in unanticipated ways. This chapter explores how the mainstreaming of robots might specifically affect privacy.

It is not hard to imagine why robots raise privacy concerns. Practically by definition, robots are equipped with the ability to sense, process, and record the world around them [Denning et al. 2008; Singer 2009, 67].[ii] Robots can go places humans cannot go, see things humans cannot see. Robots are, first and

foremost, a human instrument. And after industrial manufacturing, the principle use to which we've put that instrument has been surveillance.

Yet increasing the power to observe is just one of ways in which robots may implicate privacy within the next decade. This chapter breaks the effects of robots on privacy into three categories—direct surveillance, increased access, and social meaning—with the goal of introducing the reader to a wide variety of issues. Where possible, the chapter points toward ways in which we might mitigate or redress the potential impact of robots on privacy, but acknowledges that in some cases redress will be difficult under the current state of privacy law.

As stated, the clearest way in which robots implicate privacy is that they greatly facilitate *direct surveillance*. Robots of all shapes and sizes, equipped with an array of sophisticated sensors and processors, greatly magnify the human capacity to observe. The military and law enforcement have already begun to scale up reliance on robotic technology to better monitor foreign and domestic populations. But robots also present corporations and individuals with new tools of observation in arenas as diverse as security, voyeurism, and marketing. This widespread availability is itself problematic in that it could operate to dampen constitutional privacy guarantees by shifting citizen expectations.

A second way in which robots implicate privacy is that they introduce new points of *access* to historically protected spaces. The home robot in

particular presents a novel opportunity for government, private litigants, and hackers to access information about the interior of a living space. Robots on the market today interact uncertainly with federal electronic privacy laws and, as at least one recent study has shown, several popular robot products are vulnerable to technological attacks—all the more dangerous in that they give hackers access to objects and rooms instead of folders and files.

Society can likely negotiate these initial effects of surveillance and unwanted access with better laws and engineering practices. But there is a third, more nuanced category of robotic privacy harm—one far less amenable to reform. This third way robots implicate privacy flows from their unique *social meaning*. Robots are increasingly human-like and socially interactive in design, making them more engaging and salient to their end-users and the larger community. Many studies demonstrate that people are hardwired to react to heavily anthropomorphic technologies such as robots as though a person were actually present, including with respect to the sensation of being observed and evaluated.

That robots have this social dimension translates into at least three distinct privacy dangers. First, the introduction of social robots into living and other spaces historically reserved for solitude may reduce the dwindling opportunities for interiority and self-reflection that privacy operates to protect

[Calo 2010, 842-49]. Second, social robots may be in a unique position to extract information from people [cf. Kerr 2004]. They can leverage most of the same advantages of humans (fear, praise, etc) in information gathering. But they also have perfect memories, are tireless, and cannot be embarrassed, giving robots advantages over human persuaders [Fogg 2003, 213].

Finally, the social nature of robots may lead to new types of highly sensitive personal information—implicating what might be called "setting privacy." It says little about an individual how often he runs his dishwasher or whether he sets it to auto dry.[iii] It says a lot about him what "companionship program" he runs on his personal robot. Robots exist somewhere in the twilight between person and object and can be exquisitely manipulated and tailored. A description of how a person programs and interacts with a robot might read like a session with a psychologist—except recorded, and without the attendant logistic or legal protections.

These categories of surveillance, access, and social meaning do not stand apart—they are contingent and interrelated. For example: reports have surfaced of insurgents hacking into military drone surveillance equipment using commonly available software. One could also imagine the purposive introduction by government of social machines into private spaces in order to deter unwanted behavior by creating the impression of observation. Nor is the

implication of robots for privacy entirely negative—vulnerable populations such as victims of domestic violence may one day use robots to prevent access to their person or home and police against abuse. Robots could also carry out sensitive tasks on behalf of humans allowing for greater anonymity. These and other correlations between privacy and robotics will no doubt play out in detail over the next decade and century.

Robots That Spy

Robots of all kinds are increasing the military's already vast capacity for direct surveillance [Singer 2009]. Enormous, unmanned drones can stay aloft, undetected, for days and relay surface activity across a broad territory. Smaller drones can sweep large areas as well as stake out particular locations by hovering nearby and alerting a base upon detecting activity. Backpack-size drones permit soldiers to see over hills and scout short distances. The military is exploring the use of even smaller robots capable of flying up to a house and perching on a window sill.

Some of the concepts under development are stranger than fiction. Although not developed specifically for surveillance, Shigeo Hirose's Ninja is a robot that climbs high-rises using suction pads. Other robots can separate or change shape in order to climb stairs or fit through tight spaces. The Pentagon is

reportedly exploring how to merge hardware with live insects that would permit them to be controlled remotely and relay audio [Schachtman 2009].

In addition to the ability to scale walls, wriggle through pipes, fly up to windows, crawl under doors, hover for days, and hide at great altitudes, robots may come with programming that enhances their capacity for stealth. Researchers at Seoul National University in South Korea, for instance, are developing an algorithm that would assist a robot in hiding from, and sneaking up upon, a potential intruder. Wireless or satellite networking permits large-scale cooperation among robots. Sensor technology, too, is advancing. Military robots can be equipped with cameras, laser or sonar range finders, magnetic resonance imaging (MRI), thermal imaging, GPS, and other technologies.

The use of robotic surveillance is not limited to the military. As Noel Sharkey has observed, law enforcement agencies in multiple parts of the world are also deploying more and more robots to carry out surveillance and other tasks [Sharkey 2008]. Reports have recently surfaced of unmanned aerial vehicles being used for surveillance in the UK. The drones are “programmed to take off and land on their own, stay airborne for up to 15 hours and reach heights of 20,000 feet, making them invisible from the ground” [Lewis 2010]. Drone pilot programs have been reported in Houston, Texas, and other border regions within the United States.

Nor is robotic surveillance limited to the government. Private entities are free to lease or buy unmanned drones or other robotic technology to survey property, secure premises, or monitor employees. Reporters have begun to speculate about the possibility of robot paparazzi—air or land robots "assigned" to follow a specific celebrity. Artist Ken Renaldo built a series of such "paparazzi bots" to explore human-computer interaction in the context of pop culture.

The replacement of human staff with robots also presents novel opportunities for data collection by mediating commercial transactions. Consider robot shopping assistants now in use in Japan. These machines identify and approach customers and try to guide them toward a product. Unlike ordinary store clerks, however, robots are capable of recording and processing every aspect of the transaction. Face recognition technology permits easy re-identification. Such meticulous, point-blank customer data could be of extraordinary use in both loss prevention and marketing research.[iv]

Much has been written about the dangers of ubiquitous surveillance. Visible drones patrolling a city invoke George Orwell's *Ninteen Eighty-Four.* But given the variety in design and capabilities of spy robots and other technologies, Daniel Solove's vision may be closer to the truth. Solove rejects the Big-Brother metaphor and describes living in the modern world by invoking the work of Franz Kafka, where an individual never quite knows whether information is being

gathered or used against her [Solove 2004, 36-41]. The unprecedented surveillance robots permit implicate each of the common concerns associated with pervasive monitoring, including the chilling of speech and interference with self-determination [Schwartz 1999]. As the Supreme Court has noted, excessive surveillance may even violate the First Amendment's prohibition on the interference with speech and assembly [*United States v. United States District Court*; Solove 2007].

The potential use of robots to vastly increase our capacity for surveillance presents a variety of specific ethical and legal challenges. The ethical dilemma in many ways echoes Joseph Weizenbaum's discussion of voice recognition technology in his seminal critique of artificial intelligence, *Computers, Power, and Human Reason*. Weizenbaum wondered aloud why the US Navy was funding no less than four artificial intelligence labs in the 1970s to work on voice recognition technology. He asked, only to be told that the Navy wanted to be able to drive ships by voice command. Weizenbaum suspected that the government would instead use voice recognition technology to make monitoring communications "very much easier than it is now" [Weizenbaum 1976, 272]. Today, artificial intelligence permits the automated recognition and data mining that underpin modern surveillance.

Roboticists might similarly ask questions about the uses to which their technology will be put—in particular, whether the only conceivable use of the robot is massive or covert surveillance. As is already occurring in the digital space, roboticists might simultaneously begin to develop privacy *enhancing* robots that could help individuals to preserve their privacy in tomorrow's complex world. These might include robots that shield the home or person from unwanted attention, robotic surrogates, or other innovations for now found only in science fiction.

The unchecked use of drones and other robotic technology could also operate to dampen the privacy protections enjoyed by citizens under the law. Well into the 20th century, the protection of the Fourth Amendment of the Constitution against unreasonable government intrusions into private spaces was tied to the common law of trespass. Thus, if a technique of surveillance did not involve the physical invasion of property, no search could be said to occur. The US Supreme Court eventually "decoupled violation of a person's Fourth Amendment rights from trespass violations of his property" [*Kyllo v. United States*]. Courts now look to whether the government had violated a citizen's expectation of privacy that society was prepared to recognize as reasonable [Id.].

Whether a given expectation of privacy is reasonable has come to turn in part on whether the technology or technique the government employed was "in

general public use"—the idea being that if citizens might readily anticipate discovery, any expectation of privacy would be unreasonable. The bar for "general" and "public" has proven lower than these words might suggest on their face. Although few people have access to a plane or helicopter, the Court has held the use of either to spot marijuana growing on a property not to constitute a search under the Fourth Amendment [*California v. Ciraolo*; *Florida v. Riley*]. Under the prevailing logic, it should be sufficient that "any member of the public" could legally operate a drone or other surveillance robot to obviate the need for law enforcement to secure a warrant to do so.[v]

Due to their mobility, size, and sheer, inhuman patience, robots permit a variety of otherwise untenable techniques. Drones make it possible routinely to circle properties looking for that missing roof tile or other opening thought to be of importance in *Riley*. A small robot could linger on the sidewalk across from a doorway or garage and wait until it opened to photograph the interior. A drone or automated vehicle could peer into every window in a neighborhood from such a vantage point that an ordinary officer on foot could see into the house without even triggering the prohibition on "enhancement" of senses prohibited in pre-*Kyllo* cases such as *United States v. Taborda*, which involved the use of a telescope. Such practices greatly diminish privacy; if we came to anticipate

them, it is not obvious under the current state of the law that these activities would violate the Constitution.

One school of thought—introduced to cyberlaw by Lawrence Lessig and championed by Richard Posner, Orin Kerr, and other thoughts leaders—goes so far as to hold that no search occurs under the Fourth Amendment unless and until a human being actually accesses the relevant information. This view finds support in cases like *United States v. Place* and *Illinois v. Caballes* where no warrant was required for a dog to sniff a bag on the theory that the human police officer did not access the content of the bag and learned only about the presence or absence of contraband, in which the defendant could have no privacy interest. One can at least imagine a rule permitting robots to search for certain illegal activities by almost any means—for instance, x-ray, night vision, or thermal imaging—and alert law enforcement only should contraband be detected. Left unchecked, these circumstances combine to diminish even further the privacy protections realistically available to citizens and consumers.

Robots: A Window Into The Home

Robots can be designed and deployed as a powerful instrument of surveillance. Equally problematic, however, is the degree to which a robot might inadvertently grant access to historically private spaces and activities. In

particular, the use of a robot capable of connecting to the Internet within the home creates the possibility for unprecedented access to the interior of the house by law enforcement, civil litigants, and hackers. As a matter of both law of technology, such access could turn out to be surprisingly easy.

With prices coming down and new players entering the industry, the market for home robots—sometimes called personal or service robots—is rapidly expanding. Home robots can come equipped with an array of sensors, including potentially standard and infrared cameras, sonar or laser rangefinders, odor detectors, accelerometers, and global positioning systems ("GPS"). Several varieties of home robots connect wirelessly to computers or the Internet, some to relay images and sounds across the Internet in real time, others to update programming. The popular WowWee Rovio, for instance, is a commercially available robot used for security and entertainment. It can be controlled remotely via the Internet and broadcasts both sound and video to a website control panel.

Access by law. What does the introduction of mobile, networked sensors into the home mean for citizen privacy? At a minimum, the government will be able to secure a warrant for recorded information with sufficient legal process, physically seizing the robot or gaining live access to the stream of sensory data. Just as law enforcement is presently able to compel in-car navigation providers

to turn on a microphone in one's car [Zittrain 2008, 110] or telephone companies to compromise mobile phones, so could the government tap into the data stream from a home robot—or even maneuver the robot to the room or object it wishes to observe.

The mere fact that a machine is making an extensive, unguided record of events in the home represents a privacy risk. Still, were warrants required to access robot sensory data in all instances, robot purchasers would arguably suffer only an incremental loss of privacy. Police can already enter, search, and plant recording devices in the home with sufficient legal process. Depending on how courts come to apply electronic privacy laws, however, much data gathered by home robots could be accessed by the government in response to a mere subpoena or even voluntarily upon request.

Commercially available robots can patrol a house and relay images and sounds wirelessly to a computer and across the Internet. The robot's owner need only travel to a website and log in to access the footage. Depending on the configuration, images and sounds could easily be captured and stored remotely for later retrieval or to establish a "buffer" (i.e., for uninterrupted viewing on a slow Internet connection). Or consider a second scenario: a family purchases a home robot that, upon introduction to a new environment, automatically explores every inch of house to which it has access. Lacking the onboard

capability to process all of the data, the robot periodically uploads it to the manufacturer for analysis and retrieval.[vi]

In these existing and plausible scenarios, the government is in a position to access information about the home activities—historically subject to the highest level of protection against intrusion by the government [*Silverman v. United States*]—with relatively little process. As a matter of constitutional law, individuals that voluntarily commit information to third parties lose some measure of protection for that information [*United States v. Miller*]. Particularly where access is routine, such information is no longer entitled to Fourth Amendment protection under what is known as the "third-party doctrine" [Freiwald 2007, 37-49].

Federal law imposes access limitations on certain forms of electronic information. The Electronic Communications Privacy Act lays out the circumstances under which entities can disclose "electronic communications" to which they have access by virtue of providing a service [18 USC § 2510]. How this statute might apply to a robot provider, manufacturer, website, or other service, however, is unclear. Depending on how a court characterizes the entity storing or transmitting the data—for instance, as a "remote computing service"—law enforcement could gain access to some robot sensory data without recourse to a judge.

Indeed, a court could conceivably characterize the relevant entity as falling out of the statute's protection altogether, in which case the service provider would be free to turn over details of customers' homes voluntarily upon request. Private litigants could also theoretically secure a court order for robot sensory data stored remotely to show, for instance, that a spouse had been unfaithful. Again, due to the jealousy with which constitutional, federal, and state privacy law has historically guarded the home, this level of access to the inner workings of a household with so little process would represent a serious departure.

Access by vulnerability. Government and private parties might access robot data transmitted across the Internet or stored remotely through relatively light legal process. But the state of current technology also offers practical means for individuals to gain access to, even control of, robots in the home. If, as Bill Gates predicts, robots soon reach the prevalence and utility that personal computers possess today, less than solid security could have profound implications for household privacy.

Recent work by Tamara Denning, Tadayoshi Kohno, and colleagues at University of Washington has shown that commercially available home robots are insecure and could be hijacked by hackers. The University of Washington team researchers looked at three robots—the WowWee Rovio, the Erector

Spykee, and the WowWee RobotSapien V2—each equipped with cameras and capable of wireless networking. The team uncovered numerous vulnerabilities. Attackers could identify Rovio or Spykee data streams by their unique signatures, for instance, and eavesdrop on nearby conversation or even operate the robot.[vii] Attacks could be launched within wireless range (e.g., right outside the home) or by sniffing packets of information traveling by Internet protocol. A sophisticated hacker might even be able to locate home robot feeds on the Internet using a search engine [Denning et al. 2009].[viii]

The potential to compromise devices in the home is in a sense an old problem; the insecurity of webcams has long been an issue of concern. The difference with home robots is that they can move and manipulate, in addition to record and relay. A compromised robot could, as the University of Washington team points out, pick up spare keys and place them in a position to be photographed for later duplication. (Or it could simply drop them outside the door through a mail slot.) A robot hacked by neighborhood kids could vandalize a home or frighten a child or elderly person. These sorts of physical intrusions into the home compromise security and exacerbate the feeling of vulnerability to a greater degree than was previously feasible.

Robots As Social Actors

The preceding sections identified two key ways in which robots implicate privacy. First, they augment the surveillance capacity of the government or private actors. Second, they create opportunities for legal and technical access to historically private spaces and information. Responding to these challenges will be difficult, but the path is relatively clear from the perspective of law and policy. As a legal matter, for instance, the Supreme Court could uncouple Fourth Amendment protections from the availability of technology, hold that indiscriminate robotic patrols are unreasonable, or otherwise account for new forms of robotic surveillance.

The Federal Trade Commission, the primary federal agency responsible for consumer protection, could step in to regulate what information a robotic shopping assistant could collect about consumers. The Commission could also bring an enforcement proceeding against a robot company for inadequate security under Section 5 of the Federal Trade Commission Act (as it has for websites and other companies). Congress could amend the Electronic Communications Privacy Act to require a warrant for video or audio footage relayed from the interior of a home. As of this writing, coalitions of non-profits and companies have petitioned the government to reform this Act along a number of relevant lines.

Beyond these regulatory measures, roboticists could follow the lead of Weizenbaum and others and ask questions about the ethical ramifications of building machines capable of ubiquitous surveillance. Roboethicists urge formal adoption by roboticists of the ethical code known as PAPA (privacy, accuracy, intellectual property, and access) developed for computers [Veruggio and Operto 2008, 1510-11]. Various state and federal law enforcement agencies could establish voluntary guidelines and limits on the use of police robots. And robotics companies could learn from Denning and her colleagues and build in better protections for home robots such that they could not be as easily compromised by hackers.

This section raises another dimension of robots' potential impact on privacy, one that is not as easy to remedy as a legal or technical matter. It explores how our reactions to robots as social technologies implicate privacy in novel ways. The tendency to anthropomorphize robots is common, even where the robot hardly resembles a living being. Technology forecaster Paul Saffo observes many people name their robotic vacuum cleaners and take them on vacation. Reports have emerged of soldiers treating bomb-diffusing drones like comrades and even risking their lives to rescue a "wounded" robot.

Meanwhile, robots are increasingly designed to interact more socially. Resemblance to a person makes robots more engaging and increases acceptance

and cooperation. This turns out to be important in many early robot applications. Social robots will be deployed to care for the elderly and disabled, for example, and to diagnosis autism and other issues in children. They need to be accepted by people in order to do so. At the darker end of the spectrum, some roboticists are building robots with an eye toward sexual gratification; others predict that "love and sex with robots" is just around the corner [Levy 2007]. Robots' social meaning could have a profound effect on privacy and the values it protects, one that is more complex and harder to resolve than anything mentioned thus far in this chapter.

Robots and solitude. An extensive literature in communications and psychology demonstrates that humans are hardwired to react to social machines as though a person were really present.[ix] Generally speaking, the more human-like the technology, the greater the reaction will be. People cooperate with sufficiently human-like machines, are polite to them, decline to sustain eye-contact, decline to mistreat or roughhouse with them, and respond positively to their flattery [Reeves and Nass 1996]. There is even a neurological correlation to the reaction; the same "mirror" neurons fire in the presence of real and virtual social agents.

Importantly, the brain's hardwired propensity to treat social machines as human extends to the sensation of being observed and evaluated. Introducing a

simulated person (or simply a face, voice, or eyes) into an environment leads to various changes in behavior. These range from giving more in a charity game to paying for coffee more often on the honor system to making more errors when completing difficult tasks. People disclose less and self-promote more to a computer interface that appears human. Indeed, the false suggestion of person's presence causes measurable physiological changes, namely, a state of "psychological arousal" that does not occur when one is alone [Calo 2010, 835-42].

The propensity to react to robots and other social technology as though they were actually human has repercussions for privacy and the values it protects [Id., 842-49]. One of privacy's central roles in society is to help create and safeguard moments when people can be alone. As Alan Westin famously wrote in his 1970 treatise on privacy, people require "moments 'off stage' when the individual can be himself." Privacy provides "a respite from the emotional stimulation of daily life" that the presence of others inevitably engenders [Westin 1967, 35]. The absence of opportunities for solitude would, many believe, cause not only discomfort and conformity, but also outright psychological harm.

Social technology, meanwhile, is beginning to appear in more—and more private—places. Researchers at both MIT and Stanford University are working on

robotic companions in vehicles, where Americans spend a significant amount of their time. Robots wander hospitals and offices. They are, as described, showing up in the home with increasing frequency. The government of South Korea has an official goal of one robot per household by 2015. (The title of Bill Gates's op ed referenced at the outset of this chapter? "A Robot In Every Home.") The introduction of machines that our brains understand as people into historically private spaces may reduce already dwindling opportunities for solitude. We may withdraw from the actual whirlwind of daily life only to reenter its functional equivalent in the car, office, or home.[x]

Robot interrogators. For reasons already listed, robots could be as effective as humans in eliciting confidences or information.[xi] Due to our propensity to receive them as people, social robots—or, more accurately, their designers and operators—can employ flattery, shame, fear, or other techniques commonly used in persuasion [Fogg 2003]. But unlike humans, robots are not themselves susceptible to these techniques. Moreover, robots have certain built-in advantages over human persuaders. They can exhibit perfect recall, for instance, and, assuming an ongoing energy source, have no need for interruptions or breaks. People tend to place greater trust in computers, at least, as sources of information [Fogg 2003, 213]. And robotic expression can be

perfectly fine-tuned to convey a particular sentiment at a particular time, which is why they are useful in treating certain populations such as autistic children.

The government and industry could accordingly use social robots to extract information with great efficiency. Setting aside the specter of robotic CIA interrogators, imagine the possibilities of social robots for consumer marketing. Ian Kerr has explored the use of online "bots" or low-level artificial intelligence programs to gather information about consumers on the Internet [Kerr 2004]. As one example, Kerr points to the text-based virtual representative ELLEgirlBuddy, developed by ActiveBuddy, Inc. to promote Elle Girl magazine and its advertisers. This software interacted with thousands of teens via instant messenger before it was eventually retired. ELLEgirlBuddy mimicked teen lingo and sought to foster a relationship with its interlocutors, all the while collecting information for marketing use (Id.). Social robots—deployed in stores, offices, and elsewhere—could be used as highly efficient gatherers of consumer information and, eventually, tuned to deliver the perfect marketing pitch.

Setting privacy. Many contemporary privacy advocates worry that a "smart" energy grid connected to household devices, though probably better for the environment, will permit guesses about the interior life of a household. Indeed, one day soon it may be possible to determine an array of habits—when a person gets home, whether and how long they play video games, whether they

have company—merely by looking at an energy meter. This important, looming problem echoes the issues discussed above in reference to access to the historically private home.

The privacy issues of smart grids are in a way cabined, however, by the sheer banality of our interaction with most household devices. Notwithstanding Supreme Court Justice Anton Scalia's reference to how a thermal imagining device might reveal the "lady in her sauna" [*Kyllo v. United States*], the temperature to which we set the thermostat or how long we are in the shower does not say all that much about us. Even the books we borrow from the library or the videos we rent (each protected, incidentally, under privacy law) permit at most inferences about our personality and mental state.

Our interactions with social robots could be altogether different. Consumers will ultimately be able to program robots not only to operate at a particular time or accomplish specific task, but to adopt or act out a nearly infinite variety of personalities and scenarios with independent social meaning to the owner and the community. If the history of other technologies is any guide, many of these applications will be controversial. Already people appear to rely on robots with programmable personalities for companionship and gratification. Additional uses will simply be idiosyncratic, odd, or otherwise private.

In interacting with programmable social robots, we stand to surface our most intimate psychological attributes. As David Levy predicts, "robots will transform human notions of love and sexuality," in part by permitting humans better to explore themselves [Levy 2007, 22]. And even as we manifest these interior reflections of our subconscious, a technology will be *recording* them. Whether through robot sensory equipment, or embedded as an expression of code, the way we use human-like robots will be fixed in a file. Suddenly our appliance settings will not only matter, they will reveal information about us that a psychotherapist might envy. This arguably novel category of highly personal information could, as any other information, be stolen, sold, or subpoenaed.[xii]

The challenge of social meaning. Again, we can imagine ways to mitigate these harms. But the law is in a basic sense ill-equipped to deal with the robots' social dimension. This is so because notice and consent tend to defeat privacy claims and because harm is difficult to measure in privacy cases. Consider the example of a robot in the home that interrupts solitude. The harm is subconscious, variable, and difficult to measure, which is likely to give any court or regulator pause in permitting recovery. Insofar as consent defeats many privacy claims, the robot's presence in the home is likely to be invited, even purchased. Similarly, it is difficult enough to measure what commercial activities rise to the level of deception or unfairness, without having to parse human

reactions to computer salespeople. Rather than relying on legal or technological fixes, the privacy challenges of social robots will require and in depth examination of human-robot interaction within multiple disciplines over many years.

Conclusion

According to a popular quote by science fiction writer William Gibson, “The future is already here. It just hasn’t been evenly distributed yet.” Gibson’s insight certainly appears to describe robotics. One day soon robots will be a part of the mainstream, profoundly affecting our society. The preceding chapter has attempted to introduce a variety of ways in which robots may implicate the set of societal values loosely grouped under the term privacy. The first two categories of impact—surveillance and access—admit of relatively well-understood ethical, technological, and legal responses. The third category, however, tied to social meaning, presents an extremely difficult set of challenges. The harms at issue are hard to identify, measure, and resist. They are in many instances invited. And neither law nor technology has obvious tools to combat them. Our basic recourse as creators and consumers of social robots is to proceed very carefully.

Bibliography

Calo, M. Ryan, 2010. “People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship,” *Penn State Law Review* 114:809.

Denning et al., Tamara, 2009. “A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons,” *Proceedings of the 11th International Conference on Ubiquitous Computing* (September 30 – October 3).

Fogg, B.J., 2003. *Persuasive Technologies: Using Computers to Change What We Think and Do*. San Francisco, Cal.: Morgan Kauffman Publishers.

Freiwald, Susan, 2007. “First Principles of Communications Privacy,” *Stanford Technology Law Review* 3:1.

Gates, Bill, 2007. “A robot in every home,” *Scientific American* (January).

Kerr, Ian, 2004. “Bots, Babes, and Californication of Commerce,” *University of Ottawa Law and Technology Journal* 1:285.

Levy, David, 2008. *Love + Sex with Robots*. New York, N.Y.: Harper Perennial.

Lewis, Paul, 2010. “CCTV in the sky: police plan to use military-style spy drones,” *The Guardian* (January).

Reeves, Byron and Nass, Cliff, 1996. *The Media Equation*. Cambridge, Eng.: Cambridge University Press.

Shachtman, Noah, 2009. “Petagon’s Cyborg Beetle Spies Take Off,” *Wired.com* (January).

Schwartz, Paul, 2000. “Internet Privacy and the State,” *Connecticut Law Review* 32:815.

Sharkey, Noel, 2008. “2084: Big robot is watching you.”

Singer, Peter Warren, 2009. *Wired for War*. New York, N.Y.: The Penguin Press.

Solove, Daniel, 2004. *The Digital Person: Technology and Privacy in the Digital Age*. New York, N.Y.: New York University Press.

Solove, Daniel, 2007. “The First Amendment as Criminal Procedure,” *New York University Law Review* 82:112.

Veruggio, Gianmarco and Operto, Fiorella. 2008. “Roboethics: Social and Ethical Implications of Robotics,” In *Springer Handbook of Robotics*, eds. Bruno Siciliano and Oussama Khatib, 1499-1524. Berlin, Ger.: Springer-Verlag.

Weizenbaum, Joseph, 1976. *Computers Power and Human Reason: From Judgment to Calculation*. San Francisco, Cal.: W.H. Freeman and Company.

Allen Westin. 1967. *Privacy and Freedom*. New York, N.Y.: Antheneum.

Zittrain, Jonathan, 2008. *The Future of the Internet: And How to Stop It.* New Haven, Con.: Yale University Press.

Endnotes

[ii] For the purposes of this chapter, a robot is a stand-alone machine with the ability to sense, process, and interact physically with the world. The term home or personal robot is used to distinguish machines consumers might buy and from military, law enforcement, or assembly robots. This leaves out a small universe of robotic technologies—"smart" homes, embedded medical devices, prosthetics—that also have privacy implications not fully developed here. Artificial intelligence in particular, whether or not it is "embodied" in a robot, has deep repercussions for privacy, for instance, in that it underpins data mining.

[iii] This is not to minimize the privacy risks associated with smart energy grids or the "Internet of things," i.e., embedded computing technology into every day spaces and products. Information stemming from such technology can be leveraged, particularly in the aggregate, in ways that negatively impact privacy.

[iv] One of the chief benefits of Internet commerce is the ability to target messages and perform detailed analytics on advertising and website use. As several recent reports have catalogued, outdoor advertisers are finding ways to track customers in real space. Billboards record images of passerby, for instance, and change on the basis of the radio stations to which passing cars are tuned. Robotics will only accelerate this trend by further mediating consumer transactions offline.

[v] Surveillance may not automatically be lawful merely because the tools were used are available to the public. In *United States v. Taborda*, for instance, the Second Circuit suppressed evidence secured on the basis of using a telescope to peer into a home on the theory that "the inference of intended privacy at home is [not] rebutted by a failure to obstruct telescopic viewing by closing the curtains." But following the Supreme Court opinion in *Kyllo*, general availability appears to create a presumption that the tool can be used without a warrant.

[vi] This is how at least two robots—SRI International's Centibots and Intel's Home Exploring Robotic Butler—already function.

[vii] An earlier study found similar vulnerabilities in one version of iRobot's popular Roomba, which moves slowly, cannot grasp objects, and is not equipped with a camera.

[viii] As discussed above, terrorist insurgents have also hacked into military drones.

[ix] The standard explanation is that we evolved at a time when cooperation with other humans conferred evolutionary advantages and, because of the absence of media, what appeared to be human actually was. There are reasons to be skeptical of explanations stemming from evolutionary psychology—namely, it can be used to prove, multiple conflicting phenomenon. Whatever the explanation, however, the evidence that we do react in this way is quite extensive.

[x] Communications scholar Sam Lehman-Wilzig criticizes this idea on the basis that, if we treat robots like other people, we can simply shut the door on them as we do with one another in order to gain solitude. People may not consciously realize that robots have the same impact on as another person, however, and robots and other social machines and interfaces can and do go many places—cars, computers, etc.—that humans cannot.

It could also be argued that we will get used to robots in our midst, thereby defeating the mechanism that interrupts solitude. What evidence there is on the matter points in the other direction. For instance, a study of the effect of eyes on paying for goods on the honor system saw no diminishment in behavior over many weeks. Nor is it clear that people will come to trust robots in the same way they might intimates, relatives, or servants—assuming we even already do.

[xi] Of course, artificial intelligence is not at the point where a machine can routinely trick a person into believe it is human—the so-called Turing Test. The mere belief that the robot is human is not necessary in order to leverage the psychological principles of interrogation and other forms of persuasion.

[xii] This is somewhat true already with respect to virtual worlds and open-ended games. Human-robot interactions stand to amplify the danger in several ways. There is likely to be a greater investment and stigma attached to physical than virtual behavior, for instance (or so one hopes, given the content of many video games). Ultimately our use of robots may reveal information we do not even want to know about ourselves, much less risk others discovering.