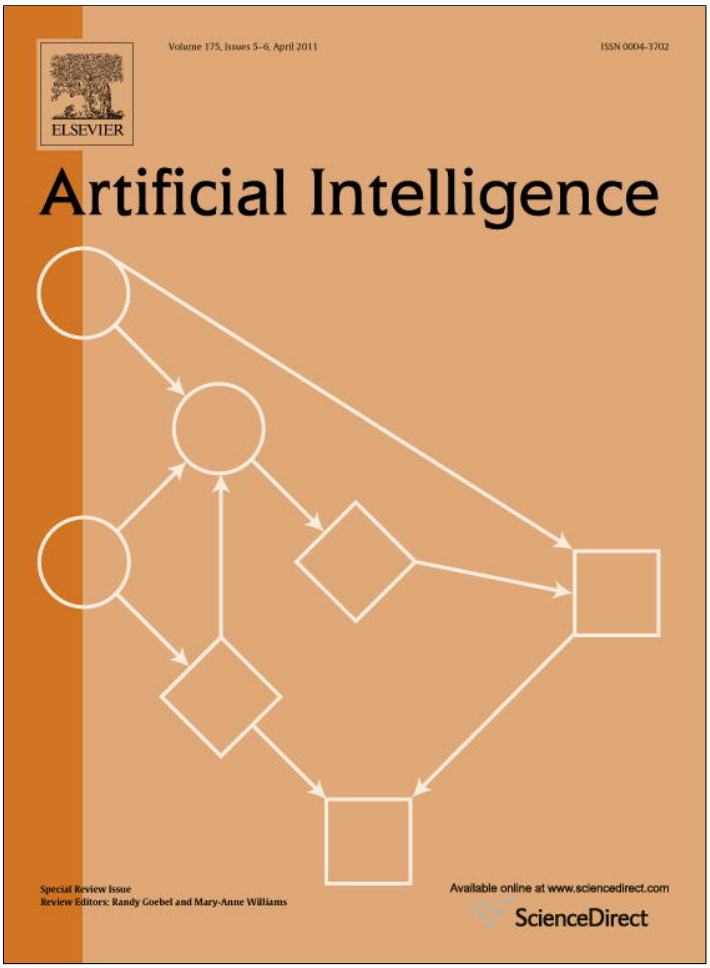

Artificial Intelligence 175 (2011) 940–941

Contents lists available at ScienceDirect

Artificial Intelligence

www.elsevier.com/locate/artint

Peeping Hals

M. Ryan Calo [1]

Crown Quadrangle, Stanford, CA, United States

ARTICLE INFO

Article history:
Received 5 September 2010
Accepted 28 November 2010
Available online 19 January 2011

ABSTRACT

Robotics and artificial intelligence hold enormous promise but raise a variety of ethical and legal concerns, including with respect to privacy. Robotics and artificial intelligence implicate privacy in at least three ways. First, they increase our capacity for surveillance. Second, they introduce new points of access to historically private spaces such as the home. Finally, they trigger hardwired social responses that can threaten several of the values privacy protects. Responding to the privacy implications of robotics and artificial intelligence is likely to require a combination of design, law, and education.

Robotics and artificial intelligence hold enormous promise. Whether it is performing task humans find impossible, dangerous, or dull; helping disadvantaged populations such as the elderly; or improving medical procedures and practice; robotics and artificial intelligence may help solve many of the worlds most intractable problems.

It is easy to see, however, why robots raise privacy concerns. Practically by definition, robots are equipped with the ability to sense, process, and record the world around them. One of the principle uses to which we have put robotics is, indeed, surveillance. Thousands of robots assist the United States military in monitoring the battlefield [1]. Robots are being field tested around the world by law enforcement for border and other domestic surveillance. Private entities increasingly lease and operate unmanned drones for security and other purposes.

Robots confer a number of advantages over human observers. They can seen things humans cannot see, go places humans cannot go. There are tiny robots that can perch on a windowsill. There are large robots that can hover thousands of feet above unseen. There are robots that can climb the sides of buildings. Robots are under development that can flatten themselves to squeeze through narrow spaces. In addition to recording standard video and audio, moreover, many robots come equipped with sensory capacities far beyond those of a human observer.

Artificial intelligence also supports surveillance. In 1976, artificial intelligence pioneer Joseph Weizenbaum questioned why the Department of Defense was funding “three or four major projects in the United States devoted to enabling computers to understand human speech” [2]. Weizenbaum could think of “no pressing human problem” that voice recognition would solve. “But such listening devices,” he noted, “could they be made, will make monitoring of voice communications very much easier than it is now.”

Today, techniques of artificial intelligence make possible an array of wonderful of products and services, including helping the deaf to hear and predicting the outbreak of disease. But these techniques also underpin all manner of sophisticated data mining. It would hardly be possible for humans to sift through the billions of communications or data points contemporary society generates without neural networks, genetic algorithms, or other applications. As Weizenbaum speculated: “Perhaps the only reason that there is very little government surveillance in many countries of the world is that such surveillance takes so much manpower.” Artificial intelligence helps supply this missing “manpower.”

E-mail address: rcalo@stanford.edu.

[1] Director, Consumer Privacy Project, Center for Internet and Society, Stanford Law School. Co-Director, Committee on Artificial Intelligence and Robotics, Section of Science and Technology, American Bar Association. This essay was adapted from M. Ryan Calo, “Robots and Privacy,” in *Robot Ethics: The Ethical and Social Implications of Robotics* (Patrick Lin, George Bekey, and Keith Abney, eds.) (Cambridge: MIT Press, forthcoming).

0004-3702/$ – see front matter
doi:10.1016/j.artint.2010.11.025

There is a synergy between artificial intelligence and robotics: smarter programs increase the capacity of robots to engage in surveillance. An interesting example is software that permits cooperation among robots, permitting them to monitor a location from multiple angles. Another is software that promotes 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.

Increasing the capacity to observe is just one of ways in which robotics and artificial intelligence implicate privacy in the near term. Even as they entertain, ease housework, and enhance the independence of those in need of assisted living, robots introduce new points of access to historically private 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.

No less than computers, robots connected to the Internet or an ad hoc network can be vulnerable to attack. Researchers at the University of Washington assessed the security of several commercially available robots and found they were able to compromise them remotely through multiple methods [3]. In addition to gaining access to video and audio, the researches were able to manipulate objects and guide the robot toward the objects they wanted to observed.

The government could lawfully gain access to robot sensory information—including real time audio and video—with sufficient process. And, unlike a standard security or computer camera, law enforcement could move a robot around the interior of the home in pursuit of contraband. Depending on how courts come to characterize robots and services that transmit and store robot data under federal law, private litigants may also be in a position to access robot setting and sensory information.

There are many ways to address the privacy issues of greater surveillance and access. Policy makers might impose limits on how the military or law enforcement can use robots to monitor civilians. Courts might strengthen privacy laws to protect the interior of the home or regulate techniques of data mining. Roboticists can build better security and privacy projections into new commercial products. Yet there is another sense in which robots and artificial intelligence implicate privacy that is not as easy to redress: these technologies tend to possess social meaning.

A mounting body of research suggests that people treat social machines and programs as though they were really interacting with a person [4]. Where a robot, program, or interface features eyes, a face, a voice, or other anthropomorphic features, our brains are hardwired to react as though a human were really present. (Indeed, it precisely his alarm at the way people reacted to ELIZA, the therapy program, that prompted Weizenbaum to write the seminal critique of artificial intelligence mentioned above.)

This phenomenon has at least three consequences for privacy. First, robots and "bots" could be used to interrogate, trick, or otherwise persuade people to give up information about themselves [5]. Work by communications scholar B.J. Fogg shows that computers can use all the same tactics as human persuaders—flattery, reciprocity, etc. The difference is that computers never tire and have perfect memories, among other advantages [6].

Second, robots, bots, and other social interfaces have the potential to interrupt solitude. One of privacy's central roles in society is arguably to help create and safeguard moments when people can be alone. We will not experience solitude in our homes, cars, and offices, if robots or other social technology accompanies us there. 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 colleagues, friends, and the public only to reenter the functional equivalent of having company [7].

Finally, home robots raise the possibility of what we might call "setting privacy." No one much cares how we use our dishwashers or microwaves. Our interactions with social robots, however, 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. Meanwhile, they may be recorded and preserved.

Unlike the issues of surveillance and access, the problem of social meaning admits of no obvious solution in law or policy. In many cases, the implications for privacy are subtle, complex, and arguably invited by the user—who, after all, adopted the technology willingly. Domesticating the issue of how we react reflexively to social machines and programs will take meticulous study and a combination of creative design and education. Thus, roboticists and user experience teams will have to be cognizant of the unintended impact of social design. Consumers will have to learn to be critical of non-human questions and claims and careful about entirely new categories of relationships.

Still, this is a worthwhile pursuit. The potential benefit of robotics and artificial intelligence are enormous. Deployed with care, robotics and artificial intelligence will continue to raise our collective standard of living the world over.

References

[1] P.W. Singer, Wired for War, The Penguin Press, New York, 2009.
[2] Joseph Weizenbaum, Computers Power and Human Reason: From Judgment to Calculation, W.H. Freeman and Company, San Francisco, 1976.
[3] Tamara Denning, et al., A spotlight on security and privacy risks with future household robots: Attacks and lessons, in: Proceedings of the 11th International Conference on Ubiquitous, Computing, September 30–October 3, 2009.
[4] Byron Reeves, Cliff Nass, The Media Equation, Cambridge University Press, Cambridge, 1996.
[5] Ian Kerr, Bots, babes and the californication of commerce, Ottawa Law and Technology Journal 1 (2004) 285–325.
[6] B.J. Fogg, Persuasive Technologies: Using Computers to Change What We Think and Do, Morgan Kauffman Publishers, San Francisco, 2003.
[7] M. Ryan Calo, People can be so fake: A new dimension to privacy and technology scholarship, Penn State Law Review 114 (2010) 809.