2017


Ramesh Subramanian
Quinnipiac University & Yale Law School, ramesh.subramanian@quinnipiac.edu

Follow this and additional works at: https://scholarworks.lib.csusb.edu/jitim

Part of the Computer and Systems Architecture Commons, Defense and Security Studies Commons, Other Engineering Commons, Science and Technology Law Commons, Science and Technology Studies Commons, Social Media Commons, and the Technology and Innovation Commons

Recommended Citation

This Article is brought to you for free and open access by CSUSB ScholarWorks. It has been accepted for inclusion in Journal of International Technology and Information Management by an authorized editor of CSUSB ScholarWorks. For more information, please contact scholarworks@csusb.edu.

Cover Page Footnote
I would like to express my sincere appreciation to the Editor, JITIM, as well as the reviewers for their insightful suggestions, all of which have made this a much better paper.

Ramesh Subramanian
Quinnipiac University
ramesh.subramanian@quinnipiac.edu

ABSTRACT

The rapid growth of AI systems has implications on a wide variety of fields. It can prove to be a boon to disparate fields such as healthcare, education, global logistics and transportation, to name a few. However, these systems will also bring forth far-reaching changes in employment, economy and security. As AI systems gain acceptance and become more commonplace, certain critical questions arise: What are the legal and security ramifications of the use of these new technologies? Who can use them, and under what circumstances? What is the safety of these systems? Should their commercialization be regulated? What are the privacy issues associated with the use of these technologies? What are the ethical considerations? Who has responsibility for the large amounts of data that is collected and manipulated by these systems? Could these systems fail? What is the recourse if there is a system failure? These questions are but a small subset of possible questions in this key emerging field. In this paper, we focus primarily on the legal questions that relate to the security, privacy, ethical, and policy considerations that emerge from one of these types of technologies, namely social robots. We begin with a history of the field, then go deeper into legal issues, the associated issues of security, privacy and ethics, and consider some solutions to these issues. Finally, we conclude with a look at the future as well as a modest proposal for future research addressing some of the challenges listed.

Keywords: AI, law, robotic law, security, privacy, policy, ethics, history, robots, social robots

INTRODUCTION

The rapid growth of AI systems has implications on a wide variety of fields. It can prove to be a boon to disparate fields such as healthcare, education, global logistics and transportation, to name a few. However, these systems will also bring forth far-
reaching changes in employment, economy and security. The US government has started to take notice of these developments. On May 3, 2016, the White House Office of Science and Technology Policy announced a series of four public workshops to address various questions that arise from these developments (https://www.whitehouse.gov/blog/2016/05/03/preparing-future-artificial-intelligence).

Indeed, as AI systems gain acceptance and become more commonplace, certain critical questions arise: What are the security and legal ramifications of the use of these new technologies? Who can use them, and under what circumstances? What is the safety of these systems? Should their commercialization be regulated? What are the privacy issues associated with the use of these technologies? What are the ethical considerations? Who has responsibility for the large amounts of data that is collected and manipulated by these systems? Could these systems fail? What is the recourse if there is a system failure?

These questions are but a small subset of possible questions in this key emerging field. It would be impossible to address all of these questions in a single project or paper. Therefore, in this paper, we focus our attention primarily on the legal questions that relate to the security, privacy, ethical, and policy considerations of one of these types of technologies, namely social robots.

To set the context we first provide a brief introduction to history and developments in AI that have led to the current interest in social robots. The history and origins of AI, its emergence as a ‘field,’ early successes and failures, and the more recent resurgence provide a useful background. We then focus on the history of social robots, a technology that is increasingly becoming prevalent in quotidian society. Following that we discuss issues and challenges connected with social robots, focusing mainly on legal issues with respect to the security, privacy, ethical and policy aspects of this technology. Finally, we conclude with a look at the future as well as a modest proposal for addressing some of the challenges listed.

The methodology used is a combination of historical and qualitative research. The qualitative research focuses primarily on analyses and opinions by non-academic and academic researchers, philosophers, as well as sociologists and technology entrepreneurs. Policy statements made by analysts, lawyers as well as government officials in the US are also considered where warranted. The primary methods for acquiring the above “data” are library research and public policy statements that have appeared in white papers, media statements and research reports.
BACKGROUND: A BRIEF HISTORY OF AI AND SOCIAL ROBOTS

The notion of building and endowing objects with intelligence has fascinated humans for a very long time. Some famous examples are: The Roman poet Ovid, who narrated the story of Pygmalion, the sculptor in *Metamorphoses* (8AD). Pygmalion created a statue of a woman so beautiful that he fell in love with it. He prayed to Aphrodite, who granted him his secret wish, which brought his statue life - enabling Pygmalion to marry his now-alive statute; and the Golem, a living creature created from dust and clay by a rabbi in Prague, who was then deployed against Roman soldiers who were attacking the city. More modern stories such as Mary Shelly’s *Frankenstein* (1818) and Carlo Collodi’s *Pinocchio* (1883) narrate human attempts to fashion living beings out of inanimate objects.

Moving forward to the mid-twentieth century, a few scientists working in disparate fields such as mathematics, psychology, engineering and economics began discussing the possibility of creating machines that could “think.” In 1950, Alan Turing published his seminal paper, “Computing Machinery and Intelligence” in the journal *Mind* (Turing, 1950), in which he described the famous *Turing Test* for the first time. In 1951, Marvin Minsky, a graduate student at Princeton, teamed up with a physics student, Dean Edmonds, to design a neurocomputer code-named SNARC (Stochastic Neural Analog Reinforcement Computer) that could simulate a rat finding its way through a maze. This was the first computer built on the principles of neural networks (Bernstein, 1981).

The contemporary field of AI was born sixty years ago in August, 1956 at the Dartmouth Artificial Intelligence Conference. The conference was organized by John McCarthy, a professor at Dartmouth University. He coined the term “artificial intelligence” while writing his proposal for the AI conference. In 1958 McCarthy and Minsky started the MIT Artificial Intelligence Lab (Chiou, Music, Sprague, & Wahba, 2001). The years following were heady times for AI. A lot was promised, and there was a good flow of government funding for AI research. However, even though several chess-playing computers were created during the next decade, there was not much by way of real progress. In 1963, *Project MAC* was set up at MIT under the direction of Robert Fano. There are conflicting theories about what the

---

1 In his 1950 paper, Alan Turing described ‘the Imitation Game,’ which eventually came to be referred to as the ‘Turing Test.’ In the Imitation Game, a computer and a human would be interrogated (using text messages) under conditions where the interrogator would not know which was, and which was not, a computer. Turing wrote that if the interrogator could not differentiate the computer from the human, then it would not be unreasonable to call the computer intelligent.
acronym “MAC” stood for. Some believe that it stood for “Machine-Aided Cognition” whereas others believe it stood for “Multiple-Access Computer,” signifying the work at MIT pertaining to time-sharing and multiple access of servers (Chiou et al., 2001). In 1962, some MIT students created a chess program that could beat amateur human chess players. In 1967, another MIT programmer Richard Greenblatt added several heuristics to an existing chess program that enabled the program it to score a very high 1400 score at a chess competition (Larson, 2016). However, beyond these examples of chess playing programs, and several research projects, useful AI was still not achievable. This led to a gradual reduction of funding for AI research. Interest in the field dropped from 1974 to 1980, and again from 1987 to 1993 (Lewis, 2014). However, during the 1980s, there was quite a lot of research in AI. The Japanese Ministry of International Trade and Industry (MITI)’s Fifth Generation Project sought to develop AI computers using massive parallelism. The first Lisp machines were developed and marketed. These allowed the development of expert system shells, which could be used to develop custom expert systems. In 1981, Daniel Hillis developed the Connection Machine at MIT. This was based on massive parallel processing. By the mid-1980s, systems that used neural networks began to be used widely. But despite these pockets of development in the field, the development of a cognitive machine remained elusive.

The big break for AI came in 1997, when IBM developed the Deep Blue supercomputer. Deep Blue had enormous processing capacity and beat expert chess players such as Gary Kasparov, the Russian Grandmaster. This was followed in 2011 by the Watson supercomputer, which won the “Jeopardy” TV quiz show (Markoff, 2011). In 2014, the “chatterbot” Eugene Goostman, developed by Vladimir Vasilov, Eugene Demchenko and Sergey Ulasen, is claimed to have passed the Turing Test, even though there is disagreement in the literature about the extent of its success (Schofield, 2014).

THE RE-EMERGENCE OF AI

Today, the Turing Test is no longer considered to be the absolute arbiter of a computer’s capabilities in behaving like a human. Freed of that requirement, the last decade has seen tremendous renewed interest in Artificial Intelligence. This stems from developments in four areas: Exponentially increased computer processor capabilities; emergence of global digital networks; advances in distributed computing (hardware and software); and the emergence of Big Data. The confluence of these developments in information technology, plus developments in psychology and sociology has brought about a new impetus to AI research. New intelligent, self-organizing and self-governing systems are becoming
prevalent in today’s business and society. Examples are social robots, driverless automobiles, autonomous flight systems (drones), and software “agents.”

SOCIAL ROBOTS: DEFINITION

The American-born British neurophysiologist and robotician William Grey Walter is recognized as the father of the Social Robots field. He published his seminal papers *An Imitation of Life* in 1950 and *A Machine That Learns* in 1951 (Walter, 1950, 1951), in which he described analog versions of an autonomous, self-learning machines nick-named *Tortoises*, due to their shape and slow movement. They were able to navigate through light signals. Robots have undergone phenomenal changes since then. Present-day Social Robots are digital, autonomous robots that are designed to independently interact and communicate with humans. They are generally built with features that resemble a humanoid form to some extent. They are capable of reasoning and independent actions, but within certain set constraints (which include safety mechanisms). In early 2015, Google was granted a patent for a robot with different personalities (Kharpal, 2015).

There are currently several definitions available for Social Robots. Some researchers even differentiate between Social Robots and Societal Robots. The former refers to those that can interact autonomously with other robots. The latter refers to those that are primary built to interact with humans (Duffy, Rooney, O’Hare, & O’Donoghue, 1999). We use the term social robots to refer to both types. Goran Bubaš and Alen Lovrenčić formalize six dimensions of interpersonal communications between artificial systems and humans, which they call “interpersonal communication competence” (ICC). They suggest that ICC should be applied in designing artificial systems that can communicate and interact with humans. The 6 dimensions of ICC are: (i) encoding and decoding, (ii) intentionality, (iii) communication effectiveness, (iv) other-orientedness, (v) expressiveness, and (vi) social relaxation (Bubaš & Lovrenčić, 2002).

Frank Hegel et al suggest that a while the social robot is perceived as a social entity, doing so would just be an anthropomorphic reaction. Instead, they suggest that a social robot should be studied with reference to form, function and context. Hegel et al define a social robot thus: “A social robot combines technical aspects as well as social aspects – but the social aspects are the core purpose of social robots.”

Kate Darling, a researcher at the MIT Media Lab, provides this general definition of social robots:

“A social robot is a physically embodied, autonomous agent that communicates and interacts with humans on an emotional level... it is important to distinguish social robots from inanimate computers, as well as from industrial or service robots that are not designed to elicit human feelings and mimic social cues. Social robots also follow social behavior
patterns, have various “states of mind,” and adapt to what they learn through their interactions (Darling, 2012).” Darling notes that social robots also mimic emotional states, exhibit adaptive behavior, and react to social cues. A good example is the Jibo, a “family robot” developed by social robotics pioneer Cynthia Breazeal, which is capable of assisting in a variety of household chores, as well as be a companion to household members (Martin, 2017).

Social robots do not necessarily have humanoid forms. They increasingly take on animaloid forms. Examples are Sony’s AIBO dog; Innovo Labs’ dinosaur Pleo; robot companions such as Aldebaran’s NAO and Pepper robots; medical and health monitoring devices like the therapeutic Paro baby seal and Intuitive Automata’s weight loss coach Autom; and household robots like Jibo (Darling, 2012). Various aspects of these robots are being studied in academic and government labs around the world. The National Institutes of Health (NIH) is studying the uses of animaloid companion robots for older people in various stages of dementia and Alzheimer’s disease (Odetti et al., 2007). The Riken-SRK Collaboration Center for Human-Interactive Robot Research (Japan) is testing the ‘RoBear’ to assist the elderly in everyday tasks (Byford, 2015). The weight-loss coach robot Autom was first developed at the MIT Media Lab in 2007 (Ackerman, 2012). At present, the MIT Personal Robots Group is one among several labs and companies that are testing robots to be personal assistants, story-telling companions, and language learning companions, etc.

SOCIAL ROBOTS AND AUTONOMY

At present there is debate on whether a social robot should be fully autonomous or semi-autonomous. Our view is that a remote controlled robot or a drone cannot be considered a social robot, as they are not fully autonomous. In a similar vein, a robotic soldier, which is really a programmed weapon of war, also cannot be considered to be a social robot. As noted by Donald Norman (Norman, 2002):

“The question is, how do you make a home robot that is autonomous, that lives by itself, that won't get stuck in corners, and doesn't have to be reminded so that it doesn't run out of power? It had to get frustrated. Being frustrated gets it out of deadlocks. If it's stuck somewhere trapped in a corner, it has intelligent algorithms trying to get it out. But if they fail, it says, "the hell with it," and goes off and does something else. It should be afraid of heights so that it doesn't fall down the stairs. It should get fatigued so that it won't wear out the battery. As its battery level gets lower, it should travel more slowly and not do some tasks. It should always make sure it’s close enough to the recharging station so that it can get back.”
ISSUES IN SOCIAL ROBOTS

To recap, social robots are capable of being fully autonomous, exhibiting affective behavior, and learning adaptively. They learn and incorporate cooperation and competition, trust and distrust, social and cultural norms. They can perform as human surrogates. The increasing prevalence of social robots in everyday society raises many questions, issues and concerns. There are numerous legal, security, and ethical implications. Since the focus of this paper is to broadly examine legal implications, focusing on security, ethical and policy implications, we look at some of the important legal cases and judgements pertaining to robots in the past, as well as important writings on the subject by legal scholars. We highlight the shortcomings of these laws and judgements and discuss the need for new legal considerations in the context of social robots.

To look at cases and judgements, we start by reviewing Ryan Calo’s examination of robots and American law (Calo, 2016).

ROBOT APPROPRIATION & IMPERSONATION

Robot appropriation cases refer to situations where a plaintiff brought a petition against a robot appropriating a human, or even another robot, thereby causing loss to the human arising from unauthorized publicity. Examples are the White v. Samsung, Wendt v. Host International, Inc., and Elnicky Enterprises v. Spotlight, Inc.

White v. Samsung: In the 1990s, Samsung Electronics ran an advertisement that depicted a robot which appeared to have some physical features of Vanna White, host of the TV show Wheel of Fortune, and which appeared to be hosting the show. White sued Samsung for violating her right of publicity. The 9th Circuit Court of Appeals agreed with Vanna White. The court declared that Samsung was liable, and that any other decision would go against the common law right of publicity (Calo, 2016; Casebriefs LLC., 1993).

Wendt v. Host International, Inc.: In 1995, the 9th Circuit Court of Appeals decided again on a similar case. In that case, the defendant Host International was sued by George Wendt and John Ratzenberger, who accused the company of using two robots in their airport bars named Cheers that appropriated the looks of Norm and
Cliff (played by Wendt and Ratzenberger), who were bar-buddies in the TV show *Cheers*. The plaintiffs accused Host International of violating their right of publicity. The court again ruled in favor of Wendt and Ratzenberger (Calo, 2016; Ninth Circuit Court of Appeals, 1995).

*Elnicky Enterprises v. Spotlight, Inc.*: This 1981 case precedes the previous two. Here, Elnicky Enterprises, which had developed a robot nick-named Rodney, sued Spotlight Presents, Inc., for developing an exact replica named Walter Ego. Judge Charles Brieant of the US District Court of Manhattan agreed with Elnicky’s claims and ruled in its favor.

These three cases deal with the question of robot impersonation of humans and other robots. Even though the robots in question were prior to the development of social robots, this could well happen with social robots, too. So the question is whether a social robot, which can be imbued with personality, be allowed to impersonate other robots or other humans.

Criminal impersonation, under the US legal system, is illegal, but governed by state laws, and thus may vary slightly from state to state. For example, the Connecticut Senate Bill No. 98 states criminal impersonation happens when the person impersonating (Senate-State of Connecticut, 2011):

1. Impersonates another and does an act in such assumed character with intent to obtain a benefit or to injure or defraud another
2. Pretends to be a representative of some person or organization and does an act in such pretended capacity with intent to obtain a benefit or to injure or defraud another
3. Pretends to be a public servant other than a sworn member of an organized local police department or the Division of State Police within the Department of Public Safety, or wears or displays without authority any uniform, badge or shield by which such public servant is lawfully distinguished, with intent to induce another to submit to such pretended official authority or otherwise to act in reliance upon that pretense
4. With intent to defraud, deceive or injure another, uses an electronic device to impersonate another and such act results in personal injury or financial loss to another or the initiation of judicial proceedings against another

Social robots are unique in that they have both a digital and analog (physical) manifestation. From the earlier discussion, we see that the judges have not made any distinction between humans and robots when it comes to impersonation, even in the special case when a robot impersonated another robot. Therefore, we can conclude in this case that social robots will come under the purview of existing
impersonation statutes without any complication, as well as the common law
governing right of publicity.

ROBOT CREATIVITY & PERFORMANCE

An illustrative case pertaining to robotic performance discussed by Calo (2016) is
Comptroller of the Treasury v. Family Entertainment Centers (Leagle, 1986). In
this case, the state of Maryland’s Comptroller of Treasury decided to levy
assessments on Chuck E Cheese franchises belonging to Family Entertainment. The
reason was a law that all restaurants in the state of Maryland were required to charge
a sales tax on food, if there were a performance on the premises. Chuck E Cheese
used some robotic puppets to provide a “performance” by singing and dancing.
Chuck E Cheese filed lawsuit against the levy, arguing that the puppets were robots
and hence did not qualify as performers, as they could not do anything spontaneous.
The court agreed, and ruled that the robotic performance fell outside the scope of
the statute. As noted by Calo, the court observed:

“A] pre-programmed robot can perform a menial task but, because a pre-
programmed robot has no ‘skill’ and therefore leaves no room for
spontaneous human flaw in an exhibition, it cannot ‘perform’ a piece of
music … Just as a wind-up toy does not perform for purposes of [the
statute,] neither does a pre-programmed mechanical robot.”

However, robotic technology has reached an inflection point. Today researchers are
developing social robots that can respond to human expressions, and can undertake
creative endeavors such as acting, creating, music, and poetry writing (David, 2015;
Wright, 2005). The author and literary critic Erica Wagner recounts how, when
presented with two examples of poetry written by humans and computers, she was
able to correctly guess one, but could not guess the other. Researchers at the
Universidad Carlos III de Madrid in Spain are currently working on a project named
“Robot Imagination System” which teaches robots to develop mental models of
objects(Leber & Leber, 2013; Robotics Lab, n.d.). There are other impressive
eamples and demonstrations of creativity by robots, as reported by Martin Gayford
(Gayford, 2016). Gayford describes intelligent systems such as AARON and The
Painting Fool. The creator of the latter, Prof. Simon Colton of Goldsmits College,
London, suggests that in order for a machine or robot to be considered creative, it
should be skillful, appreciative and imaginative. Gayford notes that The Painting
Fool has made progress in all these areas.
Given these developments, it is no longer possible to state unequivocally that a robot does not have or will never have imagination or creativity. This would be even more the case when applied to social robots. Companion robots like EmoSpark (from EmoShape), Jibo and Pepper robots can detect human companions’ emotions and act accordingly (Adee, 2015). Thus, if a social robot was performing at Chuck E Cheese, the notion that it is devoid of creativity would likely become dependent on technological developments in the field. To the extent that one cannot completely argue that a social robot cannot act independently and exhibit any creativity, the judgement could well go against Family Entertainment Centers were it to come up now or in the future.

One way the courts could sort out this ambivalence is to focus on the level of autonomy that a robot is imbued with in a specific area e.g. as music composition, drawing, or similar endeavor. If a robot has reached a critical level of autonomy, then it can be considered a “creative.”

**ROBOT SURROGACY**

An important question is whether a social robot could function as a surrogate for a human. There are numerous instances where a robot has been deployed to work in environments that are not particularly safe for humans to work in. Examples include locating shipwrecks, undersea monitoring, bomb disposal, volcano, and space exploration. But there have also been some legal challenges to the validity of robots as human surrogates. An interesting case law is *COLUMBUS-AMERICA DISCOVERY GROUP, INC., Plaintiff, v. The UNIDENTIFIED, WRECKED AND ABANDONED SAILING VESSEL* (Justia Law, 1990), as noted by Calo (Calo, 2016).

In this case, The Columbia-America Discovery Group used robots to locate and gain access to the sunken wreck of *S. S. Central America*, a steamship carrying gold that sank on the Atlantic Ocean in 1857. Then the Discovery Group asked the US District Court of Eastern Virginia for complete salvage rights, and to restrict other similar salvage operations from access to the shipwreck. The court agreed, reasoning that since the robots were under full control of human operators, the Discovery Group was entitled to the request based on the “first salver rights” in maritime law (Justia Law, 1990).

However, developments in technology have enabled fully autonomous robots to search for and map the geography of the ocean floor, locate shipwrecks, and once
located, autonomously inspect and report the findings. These are akin to giving a robot an idea of its mission, and then allowing the robot to autonomously search, locate, access and inspect the wrecks. These robots are not completely under the control of human “handlers.” They may react to unforeseen circumstances using their own prior knowledge rather than depending upon human intervention. The question that arises then is whether these robots are the surrogates of the human “owners”, under complete human control (which they are not) and whether the owners can claim that the robots are their surrogates employed for a specific purpose. Another question arises when an autonomous robot sent out to map ocean floor geography decides to investigate certain phenomenon and discovers a sunken treasure ship. In this case, can the human owners claim the shipwreck based on the “first salver” principle?

Another interesting possibility is space exploration. If a fully autonomous robot is sent to a celestial object (planet, satellite, meteor, etc.) inside or outside our solar system, can the sender of that robot claim ownership if the robot lands in a particular object? At present, there is no answer to this, as there are no laws that addresses this situation. The United Nations Office of Outer Space Affairs has adopted several resolutions focused towards international cooperation and peaceful uses of outer space (UN Office of Outer Space, n.d.). But none of them address the issue of ownership claims through robotic surrogacy as of now. However, considering plans by certain space entrepreneurs to colonize other planets in the solar system, it would be appropriate to consider the laws of ownership, especially through surrogates such as autonomous robots.

**ROBOTS AND PROPERTY OWNERSHIP**

The above section naturally leads to the issue of whether robots can have rights to property ownership. In this, we look at a recent US Supreme Court Decision on *Burwell v. Hobby Lobby*. In that case, the plaintiffs (Hobby Lobby and two other private corporations sued the US Department of Health and Human Services, claiming that the department’s mandate to provide coverage for contraception violated their freedom under the Religious Freedom Restoration Act (RFRA) of 1993. The US Supreme Court agreed, recognizing that corporations are entitled to religious freedom under the First Amendment, just like actual people. Thus, corporations have the right to own property, enter into contracts, enforce contracts, and make political contributions (US Supreme Court, 2014). They can also be sued and held liable under civil and criminal law. US attorney John Frank Weaver argues that based on this reasoning, robots should have many of the rights that corporations have, such as owning property (Weaver & Henrickson, 2014), though there would
be some restrictions. Recently, the European parliament urged the drafting of rules that would govern the use and creation of robots a form of “electronic personhood,” which would also include rights to property ownership (Hern, 2017). Now if we consider social robots, which can actually be considered as human companions, we could use and even extend the reasoning whereby social robots may eventually be allowed to own property and even be considered a beneficiary in a person’s will.

**ROBOT OBJECT AND MEMORY PERMANENCE**

A critical issue pertaining to property ownership, acquisitions and retention is the notion of object permanence. While companies are generally accepted as fairly permanent entities, we do not think the same of robots. However, there is currently research underway on creating social robots that can acquire and retain memory and consciousness. A prime example is Bina 48, which is a representation of the wife of Martine Rosenblatt, CEO of Flolan Pharmaceuticals, and founder of Sirius Satellite Radio (Gary, 2015). Bina 48 has the consciousness and memory of Bina Rosenblatt, and can be a precursor of robots with memory and permanence. This also raises the issue of uploading memory and consciousness into the cloud, to be downloaded when and where necessary.

**ROBOTIC THEFT**

How do current laws apply to robots used in burglary? We see two possibilities that could occur with today’s robots in the context of burglary. The first is when the owner of a robot uses the robot to burgle. The second is when a robot belonging to an individual is co-opted by another and then used to commit burglary. We address these two scenarios, again using case laws.

The question of robotic burglary has been partly addressed by the US courts for many years, though most of them have been before the advent of the newer robots. Thus the past cases do not explicitly involve robots. For example, one case involved the use of stolen credit cards in an ATM (the stolen card being the artificial object that is used in the burglary) (*People v. Ravenscroft* (Justia Law, 1988)). In that case, the question was whether the defendant was breaking and entering to burgle the bank, even though he was just using the ATM belonging to the bank. The court decided that he was indeed breaking and entering the bank with intent to burgle. A second case (*People v. David*, 1998) involved David, the defendant, presenting a forged check to a teller of a check cashing business by placing the check in a deposit
chute. The defendant maintained that his burglary conviction should be reversed because he did not actually enter the facility (California Supreme Court, 1998). In that case also, the court ruled that David did indeed burgle the business in question, even though he did not personally enter the business.

In both of these past cases, the key point that the courts ruled on was that it was not really necessary for a person to enter a facility in order to burgle it. He/she could use a surrogate or a technology. Thus, if we consider robots as the new technology, by using this consideration, the person who uses a robot to burgle could still be convicted of burglary even if he did not enter a particular facility. This reasoning would also logically apply to telepresence robots, since they are typically used to virtually extend the presence of an individual.

The second scenario is when a compromised robot belonging to another is used to commit burglary. Here the robot can be inside an organization or facility, but could have been compromised and made to undertake actions that either directly or indirectly helps or participates in the burglary. This scenario gets complicated because the perpetrator, if caught, could plead that while he/she hacked into and gained control of an ‘internal robot,’ he/she did not actually command the robot to burgle. (Basically, the perpetrator can command the robot to undertake certain actions that could indirectly facilitate his/her criminal action). At present, we are unaware of any law that addresses this situation.

Moving to the present and near future, if we consider a social robot, the situation becomes even more murky. For instance, can a social robot, aiming to please its human companion, undertake certain actions, including burglary, if it considered it necessary? What are the rules governing such situations? Would this be a design issue? In addressing the law concerning these issue, it would be appropriate to consider surrogate liability laws, parental liability laws and accomplice liability laws.

**SURROGATE LIABILITY**

An interesting perspective is available from military law. The US military has maintained the practice of using surrogate forces in conflicts for a long time. In this scenario, it is possible that these surrogate forces commit some crimes. If that should happen, one question would focus on what legal liability does the US or its military forces face for the crimes of the surrogate forces. Captain Gregory R. Bart of the US Navy has argued that the US military forces have no legal duty to investigate or intervene against war crimes committed by surrogate forces as long
as the US forces do not directly participate in those crimes (Bart, 2014). Bart’s arguments are confirmed by the International Criminal Tribunal of the Former Yugoslavia (ICTY), thus setting an international precedent. The ICTY ruled in 2011 that individuals who provide material support (and arms) to surrogate forces are not liable for the crimes committed by those surrogates if a direct order has not been issued (ICTY, 2011).

These cases and postings from the US military seem to imply that where a surrogate commits a crime, the “owner” or employer cannot be held liable. If we assume that (social) robots are surrogate technology, and apply the military laws as precedent, then in cases where a crime such as burglary is committed by a robot, the robot’s owner is not liable for those actions, according to the precedent.

This thought is echoed in the civilian realm by legal scholar Garbiel Hallevy, who states that if the artificial entity is capable of reasoning and acting independently, and commits a crime that neither the programmer of the robot nor the user intended to happen, nor could be considered a natural probable consequence of the programmer’s coding or the user’s actual use of the robot, then the robot (or artificial entity alone is liable, not the programmer of the AI or the user/owner (Hallevy, 2010b). However, Hallevy also states that if the programmer coded the robot in a manner that allowed it to commit a crime, and the robot committed a crime that was beyond and more serious than what the programmer intended, then the natural probable consequence test would be met, and the programmer would be liable.

**PARENTAL LIABILITY**

Another perspective comes from the realm of Family Law pertaining to Parental Responsibilities. If we can assume that a social robot is akin to a child of the owner, then these laws can be considered for addressing situations where a robot, under or outside the control of the human owner, causes damage or participates in criminal acts. There exist parental responsibility laws in every state in the US. In the state of Connecticut, the *2005 Connecticut Code – Sec 52-572, Parental liability* for torts of minors states that parents and guardians of minors will be held responsible if those minors “maliciously cause damage to any property or injury to any person (Justia Law, 2005).”
ACCOMPlice LIABILITY

An accomplice is a person who encourages and aids a perpetrator in a criminal scheme. Over the years, courts have extended the liability stemming from the criminal acts of the perpetrator to the accomplice also (Hallevy, 2010a). In the case of an autonomously functioning social robot, if the robot willfully aids in a criminal act of the user or owner, while knowing that it is indeed a criminal act, then the robot becomes an accomplice to the crime and is thus as liable as the perpetrator himself. Here there could be an extended scenario, wherein one robot commits the criminal act, but gets another robot to aid the act by gaining control of the second robot. Even in this case, if we assume that the second robot has the capability for autonomous reasoning, then the second robot is indeed criminally liable.

WHAT DOES ROBOTIC LIABILITY REALLY MEAN?

Many past writings on robots, even fully autonomous robots take the view that the notion of liability does not make any sense as far as robots are concerned. In that case, what would be the appropriate consequence of a robot indulging in crime, or destroying property, indulging in vandalism, or other aggressive, unwanted and unlawful behavior? One view is to treat a robot as an assistant. In that case, if the robot software is bad or damaged, then it is likely that the robot may undertake certain actions that is unlawful. In other cases, a robot may hurt people or damage property accidentally, during its learning stages. In some cases a robot may decide to commit a crime in order to help its user/owner. Or a robot may hurt people or damage property purely as self-defense.

In all of these cases, the closest that robots come to are companies and corporations. Punishment is often meted out to corporations for wrong-doing. There are a variety of punishments to such corporations, such as fines, prohibition to operate, reparations, etc. These sorts of punishments are effective because in the end, there are people behind the corporations, who do not want to be completely incapacitated from the corporation’s actions and the resulting punishments. We could consider treating robots as companies, in which case the robot may be fines, forced to pay reparations, or forced to cease operating. For robots to be able to pay the fines, they must have some form of liability insurance that should be set up by the robot manufacturers (for damages and unlawful acts resulting from software malfunctions) and users who acquire robots as assistants (for communicating with the robots in such a manner as to encourage the robot to undertake autonomous action with a view to protecting its user/owner).
Given the above reasoning, we believe that it would be more appropriate to consider the social robot as a servant – a mostly autonomous person who nevertheless performs duties for others. If we use this reasoning, the issue of liability become a lot clearer. There are numerous case-laws and writings that focus on this issue. Under the doctrine of respondeat superior, a master is held vicariously liable for the tortious conduct of his servant committed within the scope of the servant’s employment (Brill, 1968). However, the phrase “within the scope of the servant’s employment” causes more confusion, since there is no clear sense of how far the scope could extend. Brill (1968) points to a lot of issues with the application of this phrase, but concludes with a support of respondeat superior, stating that “the employer is the one best able to absorb the injured person's losses as a risk of doing business and to pass them on to society as a whole.” The whole notion of respondeat superior will no doubt be challenged and re-examined in the future, in the context of social robots. However, we believe that this doctrine provides one of the best approaches to sort out the issue of the liability of social robots.

The above discussion primarily focused on certain important legal issues pertaining to social robots, which is the main objective and focus on this paper. In the next few sections we briefly address some of the security, privacy and ethical issues that present themselves in any consideration of social robots.

SECURITY AND PRIVACY IN SOCIAL ROBOTS

The practical issues with respect to privacy involve data protection and data transfer. These issues however do not differ too much from the security involving current networked systems. Robots constantly interact with the environments in which they operate. This involves continuous transfer of large amounts of data in and out of the system. With respect to social robots, the data is not just environmental and contextual data, but also those that pertain to the specific humans that these robots are attached to. This could include sensitive health and financial information. Thus it goes without saying that security and discreetness of social robots is obviously a very critical design imperative. It affects the safety and security of the robot as well as the individual that it is associated with, including the individual’s properties. In this context, it would probably be useful to develop security standards for social robots, which could involve biometric methods to identify “safe” humans and their commands. These are primarily what we consider to be “design issues.” In this regard, a group of robotics researchers at the University of Washington experimented with some household robots in 2009. They found that they could easily hack into the robots and control their actions (Denning,
Matuszek, Koscher, Smith, & Kohno, 2009). Based on their study, they then published a set of design questions that could be used as a template when designing social robots. The designs basically start with the purpose of the robot, and then develop a set of questions that will enable their safe development and deployment. Legal scholar Jack Balkin has proposed three “laws of robotics for the Algorithmic Society (Balkin, 2016) to address some of these legal issues:”

1. Algorithmic operators are information fiduciaries with respect to their clients and end-users
2. Algorithmic operators have public duties toward the general public
3. The central public duty of algorithmic operators is not to be algorithmic nuisances. They may not externalize the social costs of their use of algorithms onto the general public

However, Balkin’s proposal might well be overshadowed by more recent advances in robotics and algorithmic reasoning processes that bring social robots closer and closer in their likeness, capability, and adaptability to humans. As AI advances, we have algorithmic operators that are capable of enhanced reasoning, and adding new knowledge to their algorithms that resembles human learning processes. In addition to maintaining the privacy of data, there is an additional, cultural notion of privacy. Privacy in the social robotic context also involves cultural notions of privacy. As social robots become highly attuned to a human’s emotive state, they need to identify the notion of “personal space” and be able to maintain a socially and culturally acceptable, appropriate “distance” without invading the privacy of the human. This would require further research on psycho-sociology of social robots. However, the template provided by Denning et al (above) does provide us with a starting point for these considerations.

Additionally, on the issue of security, we also need to consider the risks and challenges that may emerge as we move towards “open-source” robotics. Such a development would certainly challenge ownership and responsibility concepts, and may pose additional security problems. A direct result of this development would be the co-opting of social robots by terrorists to suit their nefarious designs. This development may require global treaties and arrangements with member nations to address and curb such developments.
ETHICAL ISSUES

There is growing literature on how humans get attached to inanimate objects, such as cars and stuffed toys. For instance, in the movie *Cast Away*, Tom Hanks develops an attachment to a volleyball, and is distressed when he lets the ball float away by accident. Kate Darling reports a military exercise where a six-legged robot was being used to spot land mines. Each time the robot stepped on a mine, one of its legs would get blown off, but the robot will continue with its remaining legs. This so distressed the commander in charge that he is supposed to have termed the exercise “inhumane” and canceled it (Darling, 2012)! There are several ethical issues that are being studied or discussed with respect to the use of these social robots. One is the “real versus fake” problem. Users of these robots could, over time, lose the ability to distinguish between what is real and what is fake, and by extension, what is authentic, and what is not. Another issue is the ethicality of replacing humans with machines in areas such as elder care, child care, etc. More studies are required in what are the long term emotional effects of these replacements on humans. Another issue is manipulation of people through these social robots. If users get attached to their social robots, it becomes eminently possible for companies and other nefarious organizations to use the robots as a means to control their human companions (e.g. through advertisements, exploitative maintenance costs, etc.). Another important and much discussed emerging issue pertains to social robots being used as objects of sex. There are obviously numerous implications that arise out of this, which include the legalities of social robots as sexual objects, gender issues, child pornography, gender issues and even sexual healing and therapy. Some of these issues are discussed in a recent report issued by the Foundation for Responsible Robotics (Sharkey, Wynsberghe, Robbins, & Hancock, 2017). While this is not the main focus of this paper, we believe that the issue of robots as sexual objects, and the implications that would arise from that, will be studied more seriously in the future. What is important is the all of the above issues raise the question of regulations and public policy formulations for social robots, which will be an important subject of study and research in the near future.

CONCLUSION

In this working paper we have briefly traced the history of social robots, and raised many issues and questions that pertain to the presence and availability of social robots in society. We have looked at the ramifications of social robots from many angles: Design issues; security and privacy issues; ethical issues, and most importantly, legal issues. The list issues are not by any means complete or resolved.
At present several researchers from various disciplines are working on some of the above questions, in order to get some answers. These researchers have primarily come from the fields of computer hardware, algorithm design, human computer interaction or HCI, law, psychology, sociology and ethics. To this mix, we could add businesses. It is quite likely that in the future, business organizations would be the biggest beneficiaries of social robots – for advertising, data mining, automating and basic operational decision-making. We hope that this paper will help researchers interested in the emerging field of social robots to understand some of the issues, and formulate solutions to these issues. A US attorney John Weaver puts forth a case for giving robots the following rights and obligations (Weaver & Henrickson, 2014):

1. The right to enter into and perform contracts
2. The obligation to carry insurance
3. The right to own intellectual property
4. The obligation of liability
5. The right to be a guardian of a minor

To this list, we would also add the right of a social robot to be the guardian and companions of invalid persons and senior citizens, keeping in mind that many of the above “rights and obligations” are already accorded to corporations under US laws and court decisions.

We also realize that this paper has shortcomings – most important of which is the focus on US laws and a general focus on US-related issues when discussing social robotics. We are aware that many countries in the EU are similarly studying the issues raised by the emergence of robots and social robots. The Policy Department of the European Parliament has recently published a report titled “European Civil Law Rules in Robotics,” with the aim of providing information on the legal and ethical issues raised by these new technologies (Directorate-General of Internal Policies, 2016). Other nations may soon add their own studies, reports and laws.

We thus believe that the emerging field of robots, especially social robots, has the potential to change the world and the legal, social and ethical constructs that we currently know and adhere to. In the near future, we may have to share the world with the new entity that would possess superior knowledge management and processing power, reasoning capabilities, physical strength and adaptability. It is therefore important for researchers in disparate fields to focus more attention to the global rise of this new entity.
REFERENCES


