Chapter 9
Trustworthiness of Autonomous Systems

S. Kate Devitt

9.1 Introduction

Humans are constantly engaged in evaluating the trustworthiness of humans and systems. Effective robots and Autonomous Systems (AS) must be trustworthy. Understanding how humans trust will enable better relationships between human and AS. Trust is essential in designing autonomous and semi-autonomous technologies, because "No trust, no use" [80]. Additionally, rates of usage are proportionally related to the degree of trust expressed [54]. Hancock et al. [37] argue that trust begets reliance, compliance and use. However, humans do already rely on systems they do not trust. Consider the unreasonable privacy policies agreed to by users to access services via apps, websites and cloud services [90]. Because privacy policies can be changed at any time, private data may be sold by organisations for profit without explicit consumer consent or even awareness. Consumers can find the benefits of the services to enhance their lives and productivity too strong to resist. In these situations, people rely on systems they do not trust and are not trustworthy. People know that their data may be shared for corporate interests. People know that they have signed away rights on their own images, etc. by using these services. As more services operate without human decision makers yet offer irresistible perks, humans may increasingly rely on untrusted AS to decide for them. Instead of trust, it may be better to consider human reliance on other humans and systems as a measure of risk aversion–of which trustworthiness remains a significant part.

S. Kate Devitt (✉)
Robotics and Autonomous Systems, School of Electrical Engineering and Computer Science, Faculty of Science and Engineering, Institute for Future Environments, Faculty of Law, Queensland University of Technology, Brisbane, Australia
e-mail: kate.devitt@qut.edu.au

H. A. Abbass et al. (eds.), *Foundations of Trusted Autonomy*, Studies in Systems, Decision and Control 117, https://doi.org/10.1007/978-3-319-64816-3_9

9.1.1 Autonomous Systems

AS can be robots, AI programs or software that operate without human control. AS are made by teams of engineers, designers, mathematicians, and computer programmers to serve a human need. AS actions and decisions are made by complex hierarchical processes balancing the uncertainties of cross modal inputs such as cameras, microphones, tactile responders with internal representations such as maps, directives and event memories. AS execute functions such as actively selecting data, transforming information, making decisions, or controlling processes without inputs [54] (p. 50). AS are defined in contrast with automated systems and manual systems. Automated systems are largely deterministic to achieve predefined goals. Classic automata such as Japanese karakuri demonstrate complicated, nevertheless predictable behaviours [1]. In contrast, AS learn and adapt in their environments rendering their actions more indeterminate over time [36, 80]. Advanced AS may be capable of executive functions such as planning, goal-setting, rule-making and abstract conceptualisation. An 'autonomous system' can refer to a subset of functions within a larger functional system or refer to the superset of functions undertaken by an agent or machine. Regardless of the scope of functions of an autonomous system, it is important that AS operate without human control.

9.1.2 Trustworthiness

Trustworthiness is a property of an agent or organisation that engenders trust in another agent or organisation. Trust is a psychological state in which a person makes themselves vulnerable because they are confident that other agents will not exploit them [68]. Trust is also a social feeling of mutual confidence that increases the efficiency of systems, allowing adaptations to externalities and uncertainties [4]. Trust, like empathy, truth telling and loyalty lubricates social interactions. Humans depend on flexible cooperation with unrelated group members that rely on trust [89]. Thus, social success relies both the evaluation of the trustworthiness of others and the presentation of oneself as trustworthy [23].

We can distinguish between the trust we place in individuals, and the general trust we have in our society that affects how we make decisions more broadly, e.g. Adam Smith [87] in the *Wealth of Nations* noted that a merchant is more comfortable trading within their own society because they can "know better the character and situation of the persons whom he trusts." Empirical literature has linked improved trust with more efficient public institutions, greater economic prosperity, self-reported health and happiness across many societies using a range of statistical techniques (see [16]). Within a Nation or society, trust is quite heterogeneous between individuals. Surveys on whether subjects trust a generic person—measured on a scale between 0 (no trust at all) and 10 (fully trusted)—find large interpersonal differences [14]. Economic productivity peaks when the average citizen rates a generic person a '7' level of

trust-a fairly high level of trust. Pessimists trust too little and give up opportunities too often. Optimists trust too much and get cheated more frequently. How does this trust research relate to AS? Do economic models apply to designing trustworthiness in AS? Should we create trustworthy systems to engender a '7' level of trust matching optimum human economic performance? That is to say, if we test the trustworthiness of autonomous-human interactions, should we aim to replicate the trust metrics found between people or some other measure?

It is important to acknowledge that trust is a complex phenomena and has been defined differently depending on the discipline [78]. Economists consider it calculative [99] or institutional [70]. Psychologists focus on the cognitive attributes of the trustor and the trustee [77, 96]. Sociologists find trust within human relationships [33]. Understanding the way humans conceive of and act regarding trust is critical to ensure the success of trusted AS. To bring different approaches under a single framework for investigation, this chapter will examine trustworthiness with three questions:

1. Who or what is trustworthy?-metaphysics
2. How do we know who or what is trustworthy?-epistemology
3. What factors influence what or who should we trust?-normativity

Building trustworthy autonomous systems requires understanding trust in human-human relationships and human-AS interactions. A research program on trusted AS ought to incorporate mental models informed from cognitive science to better understand and respond to human thoughts and behaviour. An example of such a research program is the recent work programming a robot with ACT-R/E [49, 94], an embodied extension of the ACT-R [3] cognitive architecture. The ACT-R/E implementation takes features of human cognition, such as segmenting time into events and narrative explanation to bring meaningfulness and trust to robot-human relationships. But, it is just one of many promising frameworks to align AS with human cognition. This chapter considers a range of theories of trust to influence the design trustworthy autonomous systems.

9.2 Background

The Fukushima Daiichi nuclear power plant disaster stemming from the Japanese earthquake and tsunami in March 2011 motivated DARPA to develop the Robotics Challenge (DRC) in 2012. Immune to radiation damage, Japan could have used robots to help rescue people, or go into the Fukishima power plant to turn off valves, investigate leaks or structural damage. Yet after decades of robot research and development Japan did not have a rescue robot. Where was the real Astroboy [1, 60]? Humanoid Robotics Project (HRP)-2 was functionally designed to assist people in construction, dangerous environments and home [47] but did not have the operational capacities to help when needed. In response, the DRC challenged robots to perform tasks modeled on the context of urban search and rescue (USAR) and

industrial disaster response task domains [105]. Tasks were real-world anthropomorphic manipulation and mobility; controlled by automated interfaces and teleoperation. Challenges included obstacles such as opening a door, turning a valve, driving a car, and walking over a pile of chaotic bricks. The first robots to attempt the challenge failed miserably. They almost all fell over or were unable to complete tasks so simple for humans. The DRC robots were not even autonomous-actions were manually controlled by teams.

Thus, despite early optimism that robots would be capable of performing human-level tasks by 2015, machines are still far from achieving this goal. Very basic tasks still require supervisory human control from one or more operators. Complex environments such as USAR, require continuous direct control by multiple operators. Engineering autonomy in robots requires more research in both pragmatic design and societal implications. Trust will emerge from evidence-based control interface design that accommodates multiple control paradigms of the robot and the user [105].

Even though the DARPA challenge remains difficult to accomplish, AS are already being depended upon in our lives, from our adaptive smart phones [56], to off shore oil rig drilling programs [34]. Self-driving modes in cars (see [91, 100]), mining trucks [82] and buses [76] are already in use. Now is the time to understand the metaphysical, epistemological and normative dimensions of trust and trustworthiness so that we can build, use and thrive with AS.

9.3 Who or What Is Trustworthy?

Who or what is trustworthy? In this section I consider what sort of property trustworthiness is and the sorts of components a trusted AS might comprise of. Trustworthiness might be an intrinsic property of an agent similar to height, or a relational property similar to tallness. Perhaps a robot that survives the apocalypse, like WALL-E [61] is trustworthy due to intrinsic moral virtues such as charm, cheeriness and helpfulness, even if there are no other humans or robots to trust him? Or WALL-E is trustworthy when compared to other robots such as EVE programmed to obey directives. Trustworthiness might be a substantial property-an independent particular-or a dispositional property-the capacity of an object to affect or be affected by other things. The classic example of a dispositional property is fragility. A vase is fragile because it breaks easily. A dispositional account might suppose that a person is trustworthy because they speak truthfully or act reliably with others. It might be thought that trustworthiness is both a dispositional and relational property established by the subjective judgment of one agent X of another agent Y in virtue their shared spatio-temporal interactions. For example, an employee goes through a three month probation period or a solder undergoes basic training to build their reputation with a Drill Sergeant or manager. The graduating employee or solider are deemed trustworthy for a prescribed set of activities with a particular group of people in a specific context. Note that any trustworthiness ascribed to an individual due to these processes pertains to that domain of actions. It's not clear how generalizable or

transferable trustworthiness is. At least an argument needs to be made to demonstrate the transferability of trustworthiness across domains.

What is interesting about Trustworthiness understood as a dispositional and relational property is that it can be established by combining judgments from multiple agents, such as through peer assessment [58]. In this way, an IT device can be judged trustworthy through a network of sensors using a reputation-checking algorithm. For example, beacon nodes on Wireless Sensor Networks can be evaluated on whether they are providing accurate location identification by 1-hop neighboring nodes [88]. Autonomous trustworthiness-evaluation and -judgment is important when networks are vulnerable to malicious interference. Indeed, trustworthiness evaluation programs are considered increasingly important with the proliferation of autonomous systems connected via the Internet of Things (IoT) (see [17, 83, 104]).

If the dispositional and relational account of trustworthiness is right, then what dispositional properties does it consist of? In the preceding paragraphs I suggested that a person might be trustworthy because they speak truthfully or act reliably. Let's look at these ideas more closely.

Central to the notion of trustworthiness is reliability and accuracy. So, an AS is trustworthy if we can *rely* on it being *right*. For example, a binnacle compass is trustworthy if a sailor can rely on it to accurately adjust to the rise and fall of the waves and orient to magnetic north [7]. If a sailor navigates to the wrong shore, she might wonder if her compass has become unreliable and thus she ought not trust it. Perhaps ferrous nails have been used that pull the needle away from true readings and the binnacle compass's reliability compromised?

Is trustworthiness more than reliability? How do properties such as adaptability meet reliability? For example, the trustworthiness of a rescue dog might be its capacity to adapt to severe conditions, such as digging through an avalanche to find a stranded person, even if the dog has never encountered such an environment. Adaptability is not an orthogonal trait, but a higher order reliability. In this case, we rely on the dog to be adaptable in unusual, unexpected or changing conditions. The trustworthiness of people, creatures and machines is related to the reliability of their capacities and functions in domains of differing complexity and uncertainty.

Is trustworthiness also about redundancy? We know that AS will not be perfectly safe. There will be hardware failures, software bugs, perception errors and reasoning errors [27]. Aerospace and military operations build in an expectation of failure into design to enable trust. For example, Boeing 747's only need a single engine to fly, yet are equipped with four engines to ensure redundancy [22]. The Space Shuttle program used five identical general purpose digital computers [85]. Four of these computers operated as a redundant set and the fifth calculated non-critical computations. The anticipation of failure and the deliberate engineering of multiple systems in avionic engineering makes these systems more reliable and hence more trustworthy. Still, is there more to trust than reliability?

Philosophers have traditionally differentiated reliability and trust. While reliability is necessary for trust, it isn't sufficient. Reliability is a property of machines and inanimate objects, where as trust occurs between conscious agents. For example, we rely on a shelf to hold books, but do we *trust* the shelf [39]? Fully-fledged trust

seems to involve reliability *and* psychological components such as the ability to apologise if we let people down, if we fail to do as we said we would. A shelf has no attitudes towards what it does. Human trust is traditionally mentally, linguistically and rationally based rather than limited to summaries of behavior [24, 40, 48, 84]. AS are a challenge to traditional philosophical distinctions on trust because they are inanimate, in the sense that they are programed to fulfill a set of tasks within a domain and have no intrinsic care for humans and no self-driven desire to maintain their reputation. The tradition to incorporate psychological attitudes in a model of trust could either be misplaced or reconsidered to drive the design processing the age of AS.

By focusing on systems as well as people, the business management literature may provide a more suitable starting framework for building trusted AS than philosophy (for more philosophical discussion see [64]). The management two-component model of trust differentiates competence-consisting of skills, reliability and experience-and integrity-consisting of motives, honesty and character (see Fig. 9.1). Using this framework user trust in AS could be grounded in reliable operations built by high-integrity organisations.

Competence comprises of skills, reliability and experience. A person or robot can be competent and yet occasionally not have exactly the right skills for the job, or the sometimes fail to do a task within their domain and sometimes reach the limit of their experience. Competence is thought to improve when an individual learns more skills, becomes more reliable and has more experiences. Integrity can be analysed as comprising of motives, honesty and character. We trust someone who is trying their best, who is transparent about their actions and has a character that, regardless of competence, inclines them to take responsibility for their actions, be thoughtful and empathetic to others and other traits. This two-factor model of trust combines ability and ethics [19, 20, 51, 59]. Trust (T) consists of:

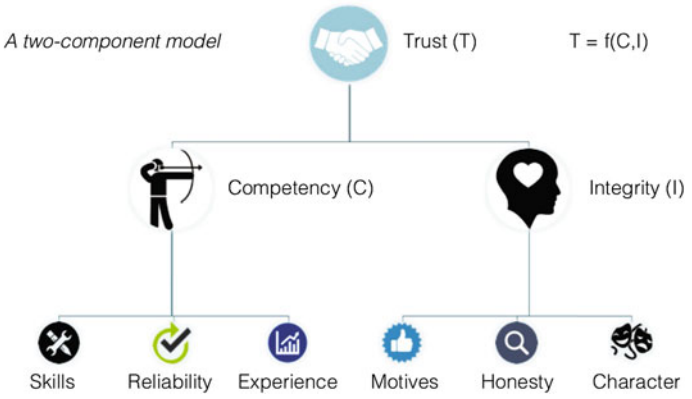

Fig. 9.1 A two-component model of trust incorporating *competence*-skills, reliability and experience-and *integrity*-motives, honesty and character [19, 20, 51, 59]

- Competence (C)
- skills (Cs)
- reliability (Cr)
- experience (Ce)
- Integrity (I)
- motives (Im)
- honesty (Ih)
- character (Ic)
- T = f(C, I)

Research suggests an asymmetry in the way trust is lost between these two factors. A single integrity failure may result in a loss of trust in the way that a single incompetent action does not [51]. People use integrity judgments to generalize across domains of a relationship, where as competence is more domain specific [20]. Additionally integrity-based trust implies a reduced threat of opportunism in a way that competence-based trust does not [59]. Trust depends on beliefs about the other's benevolent motives [103].

Notice the difference between human-human trust and human-AI trust violations. There is an interesting asymmetry between levels of competence required for humans to trust other humans versus trusting AI. Unlike human-human relationships, trust built up inductively between humans and AI can be destroyed with single instances of inaccuracy or unreliability. Consider the mistakes Google's AI made identifying vertical wavy lines as a starfish [69]. A single misidentification of a starfish can end trust in that machine learning algorithm even though it has performed well in the past. Consider the disproportionate media scrutiny of the first Tesla autopilot fatality. The Tesla flaw was due to the car's incapacity to differentiate the reflectance of light from a truck from the reflectance of the sky [86]. Even though human drivers make perceptual errors leading to crashes all the time, the Telsa fatality caused much uncertainty around whether the AI responsibly could be trusted. The Tesla case is a good example of much higher competence-based trust thresholds for AS than human operators and where a single model may not be sufficient. But, not only are competency requirements misaligned between human-humans and human-AS, but the integrity aspects of the model present a challenge for AS design.

Consider the requirement for honesty in Fig. 9.1. Engineers might correctly wonder how to communicate complex computational processes to human operators who themselves do not have the competency to understand their underlying logical operation? The data and algorithms of autonomous agents are hidden from most human stake-holders and cannot be understood even if a translation layer were added and explanations communicated in plain language. Perhaps human do not expect honesty from AS the same way they do from other humans? A question then is, whether humans *should* mistrust AS based on perceived honesty violations (I_h). Should engineers creating an AS prioritise transparency and communication of their decision-making mechanisms for trust and adoption? Should users demand them? It is important to consider that integrity components of the trust model might be appropriate for the human engineers, designers and corporate representatives of AS, but perhaps

not crucial for the systems themselves? That is, so long as human stakeholders can honestly report the technical specifications of AS to other experts such as regulators, then AS do not need to convey integrity information to users.

What about the role of motives (I_m) and character (I_c) on trusted autonomy? Sometimes humans believe AS have more psychological reality than they actually do due to clever programming. ELIZA was one of the first relational AIs designed to engender trust using simple grammatical tricks [15, 95]. Little has been developed since that could be dubbed motives or character. Merrick, Klyne and Hardhienata in Sect. 15.5 discuss the interplay between motive and reliability. They argue that lack of transparency in the motivations or experiences of an agent can reduce trust between humans and robots, as it is difficulty to gauge why a robot is behaving the way it is, and hence, whether it is trustworthy. They suggest reputational models to help multiple users know when they should trust a particular agent. However, they also note that there is very little work done that incorporates both computational models of motivation and computational models of trust.

AIs in science fiction imagine how character might affect operations. HAL from the movie 2001: A Space Odyssey [52, 53] is a malevolent AI who lacks integrity, but is fairly competent at achieving a mission-albeit his own. Deep Thought from the Hitchhikers guide to the Galaxy [2, 67] is a benevolent AI who provides answers that humans don't want to hear, such as that the meaning of life, the universe and everything is 42. AIs can have varying degrees of competence and integrity that affects how we trust them. Additionally, may be other factors in a successful model of trust to truly understand how humans will respond to extremely smart AI.

The model described in this section is the start of an investigation of what trustworthiness could be between humans an AS based on an interdisciplinary investigation. Critics have noted that the model above confuses an influencing factor and an indicator.[1] They argue that reliability is an *indicator* of competence, not an input like skills and experience that generate competence. Skills and competence are independent variables that influence competence. I argue that while reliability is not an input, it is a *property* of a trustworthy system, not merely an indicator, hence its inclusion in the model along with skills and experience. Isolating reliability from skills and experience is meant to allow for multiple ranges in skills, reliability and experience to operate independently from one another. So, a person might be a skilled carpenter with years of experience, yet be incompetent at time tm because his divorce lead him to alcoholism and unreliable behaviours. Reliability is not merely the combination of skills and experience, it requires additional features such as the adaptability and redundancy discussed above. However, the critic is right that much more work needs to done to refine and hone this model to appropriately capture the metaphysics of trustworthiness for AS. The management model is just the beginning of incorporating human factors into AS design.

[1] Many thanks to an anonymous reviewer for bringing up this distinction.

9.4 How do We Know Who or What Is Trustworthy

How do we decide whether to trust? In Sect. 9.3 the properties that establish and define trustworthiness were considered. In this section the epistemology of trustworthiness is examined-how do we know who or what is trustworthy? What are the indicators of trust? If a person claims to justifiably trust another, it indicates they have the ability and confidence to predict others' behaviour [62]. Implicit, heuristic or 'gut' indicators of trust are often grounded in physical responses and intuitions. Explicit, reflective or rational trust stems from our experience of people over time and our reasons to judge their trustworthiness. Often we do not know why we trust, we trust implicitly. Thomas Reid (1764) [75] argued that reasons could not be required for trust given that'most men would be unable to find reasons for believing the thousandth part of what is told them.' Reid's point is that humans must be justified to trust even in the absence of reasons. Consider the way we use Google maps. Many people use Google maps to get them where they need to go, without knowing how Google maps works, how their phone works or how traffic influences the instructions Google maps provides. Not only do people not know why they trust Google maps, it does not seem to concern people that they do not know why. So how do humans make trust judgments of systems and each other, and are these the same mechanisms that elicit trust in AS? This section moves through implicit and explicit justifications of trust followed by a cognitive model of trust and competence and finally a brief comment on the relationship between trustworthiness and risk.

9.4.1 Implicit Justifications of Trust

Implicit justifications of trust are preconscious, embodied trust responses developed without top-down cognitive evaluations. For example a monkey climbs a vertical structure implicitly trusting that it will improve their odds of survival against predation. Researchers know how to alter physical properties of embodied AS (i.e. robots) to engender implicit trust including how they look, sound and feel. Social robots are designed with big responsive eyes and eyebrows [12], as are mobile, dexterous and social robots (MDS) [11, 94]. Some designers have shaped robots like baby animals-such as the harp seal robot PARO [1]-and use biomimetic features such as soft skin for tactile trust [50]. The Kismet robot with human-like eyes, eyebrows and lips was designed to recognize and mimic emotions, including facial expressions, vocalisations and movement [12].

Physical actions connote trust in humans. Japanese robot designers have found cultural identification with a robot who imitates traditional 'aizu bandaisan' dance [1]. Japanese robot designers try to build trust by incorporating aspects of fictional references to helpful and social robots, such as Anime characters Astroboy and the Patlabor [1]. But, representations can be incredibly primitive and build emotional attachment, for example, humans watching 2D dots moving on a screen intuitively differentiate between animate versus inanimate movement based on how wel algorithms replicate biological behaviour [74]. Mimicry of biological behaviours can

make people empathise and be concerned for the wellbeing of robots, evidenced by viral videos of the Spot robot by Boston Dynamics being kicked and struggling to stay upright [9].

People enter into a relationship with a robot if it simulates human-like emotional and personal understanding, even though these relationships lack the authenticity of shared human meaning [95]. Entirely soft autonomous robots may bridge the authenticity divide, triggering different emotions and trust reactions than solid state robots. Consider the 3D printed soft Octobot designed to emulate a real Octopus, controlled with microfluidic logic instead of microchips [98]. Biology-inspired control systems are likely to affect trust responses.

The way AS communicate verbally and through sound can have a big impact on implicit trust. Tom Gruber (Siri Advanced Development Head at Apple) argues that people feel more trusting of Apple's Siri if she has a higher quality voice, "the better voice actually pulls the user in and has them use it more. So it has an increasing-returns effect" [56].

Physical characteristics also impact on how much humans move from empathy to revulsion when robots are like humans, but eerily not quite like humans-known as the uncanny valley [66] impacting how much people intuitively trust them. There is much research still to be done on whether AS that does not attempt human-like physical characteristics might not arouse the same empathy or emotional connection, but may still generate trust. The rise of chatbots in the tradition of Eliza is a linguistic means by which to generate disembodied trust. However, one benefit from realistic facial gestures and embodied movements of robots could be a speed advantage of conveying subtle information regarding the uncertainty of a robot's beliefs, their skepticism or their competing interests when providing an answer to human query improving integrity judgments (see Fig. 18.1). Such gestures may be implementable as avatar animations alongside text communication. The model outlined in Sect. 9.3 may also help us understand how humans implicitly trust autonomous systems in lieu of human-like physical characteristics or avatars. Consider human-drivers who trust Telsa's autopilot function. The car has no physical similarities with humans. Additionally, Telsa drivers cannot trust Tesla because they explicitly know anything about the algorithms before they set the autopilot on. Trust could come from implicit factors such as integrity or reliability (see Fig. 9.1). Integrity judgments may stem from a cult of personality around Elon Musk's extensive future vision for solar power, electric cars and sustainable colonies on Mars [26]?

9.4.2 Explicit Justifications of Trust

Trust is explicitly justified when we have reasons to rely on someone or something. These reasons might coalesce into a deductive, inductive or abductive inference based on the testimony and behaviour of an agent. The link between trust and higher order reasoning is supported by research showing that human intelligence relates to how successfully people evaluate trustworthiness [16, 21, 102]. Under this hypothesis, intelligent people foster relationships with people less likely to betray them and make

better contextual judgments to account for circumstances where trust is difficult to uphold. Explicit reasons for trust may allow more nuanced and accurate trust judgments than relying on gut feelings or intuition.

Faulkner [25] argues that though we need reasons to trust an agent generally, we do not need reasons to justify *particular* statements from that agent. Our reasons to trust are based on evaluations of a *general* trustworthiness of an agent [24, 39–41, 63]. After all, the boy who cried wolf was not trusted in the end because he had a history of false testimony even though he was correct in the final instance. A trustworthy reputation for Y built up inductively with X can be shared quickly via testimony to other agents P, Q and R etc... Thus, the value of a trustworthy reputation is not only the ability of X to act based on information provided by Y, but its *transferability*, that is, secondary agents P, Q and R, are justified to trust Y *iff* they trust X without themselves needing prior interaction with Y. The transferability of a trustworthiness judgment increases the effectiveness and efficiency of social relationships and information systems.

But, does increased efficiency dangerously increase risk? Hume rejected testimony as a source of justification for trust [43]. He thought that a hearer was justified to trust based only on their *personal* observations of the speaker's history of truth-telling plus inductive inference from those observations [29]. Hume's reluctance to accept other people's pronouncements demonstrates the subtly and context-sensitivity of trust relationships. An AS might be trustworthy for native English speakers, but break down when deployed in mixed language context. Or an AS learns how to operate with a Platoon, but must be re-skilled each time it interacts with a new human team.

Highly complex AS are a problem for explicit justifications of trust. Because if reasons are required for trust, then perhaps no individual has sufficient reasons to make such a judgment? Take the job of calibrating a ScanEagle unmanned aircraft with hyperspectral imagery sensors to map coastal areas [42]. One individual might verify the location and ensure the imagery sensors are operating correctly but be unable to evaluate the hyperspectral map. The point is that no one operator may know or vouch for all components, mechanisms and physical properties that comprise a complex AS. A key difference between human-human trust and human-As trust is the complexity and difficulty of a single agent-agent dyad relationship. I propose that instead of relying on individual testimony AS be judged trustworthy by teams and groups that are themselves deemed to be trustworthy within the domain. Groups may include (but are not limited to):

1. Regulatory agencies responsible for issuing parameters of safe operation including physical construction and operational algorithms, operator licensing, maintenance, consumer safety.
2. Institutions and companies designing and building AS.
3. Cohesive teams of staff responsible for successful operations.
4. Environmental conditions conducive to operational success.

Hume's framework could still be useful within a more layered and complicated system of establishing explicit trust. A Human regulatory framework means that an

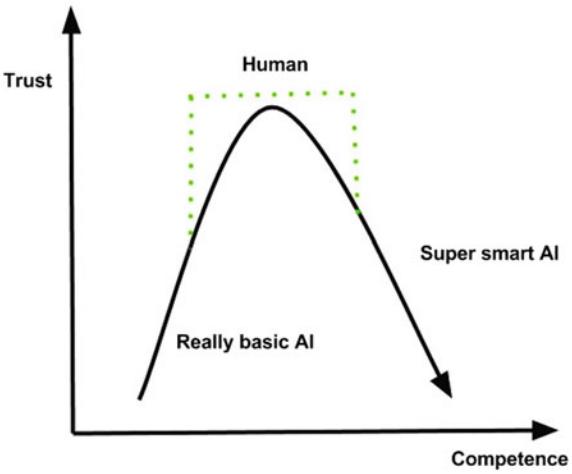

Fig. 9.2 Model of trust and competence where human levels of competence yield the highest trust and trust is reduced at sub-human and super-human levels

individual is justified in trusting an AS in virtue of their background knowledge of the past veracity of regulators, companies and staff plus inductive inference from those beliefs to a current instance. However, induction remains a significant problem for fast evolving AS. New AS may be made by cohesive and trustworthy teams, yet not have sufficient inductive evidence to generate warranted trust in their safe operation. This may be true, even though an individual knows that a particular aircraft company has a history of trustworthiness and that the regulatory bodies have a history of safe aircraft policies. In cases where innovation is radical and complex, trustworthiness needs inductive and abductive arguments-inference to the best explanation-to justify operations. An individual or organisation should devise an individualized set of weighted factors that together render a trust or not-trust threshold for a particular AS.

9.4.3 A Cognitive Model of Trust and Competence

Considering both intrinsic and extrinsic forms of justification, is there a linear relationship between competence and trust (holding integrity constant)? I propose that trust and competence forms more of a quadratic relation for trust. We build trust as agents become more competent. We reserve a pinnacle of trust at a human level of competence, and then trust declines as humans or machines exhibit competence at the outlier or far beyond ordinary human capacity to understand it-see Fig. 9.2. This model needs empirical testing, but I think the burden of proof is on the developers of AS to demonstrate how trust can be retained or improved as competence surpasses human capabilities and understanding. Such a justification may arise via reputational justifications as specified in Sect. 9.4.2.

To appreciate the impact of outlier competence, consider the AlphaGo game played against leading Go player Lee SeeDol in 2016 [65]. In move 37, Match 2, AlphaGo-a machine learning AI-placed a single black stone on the board that shocked the human player Lee SeeDol so much that he immediately left the table. This move was incomprehensible at a top Go playing level. What this move revealed was that humans sometimes do not understand why an AI acts in order to evaluate it. This is relevant because each competitor playing Go must presume the capacity in their opponent (human or AI) and use game play to build theories to explain strategies and mistakes of their opponent. When playing another human, Go players might overtly inquire about the opponents Go background (how old were they when they begin playing? How much have they played? Who have they played against? What books have they read? What teachers have they had? What sort of handicap do they have? etc.). Players watch their opponents actions, not only the stones placed, but the manner of their placement, and the ultimate destination on the board. Each move can be evaluated in the immediate context of the game, but also in forming what Nelson Goodman [32] describes as *overhypotheses* about their opponents style, learning journey, preferences, beliefs and desires. Players use these overhypotheses to predict what an opponent will do, then use these predictions to design their own strategies to counteract them. In terms of outcome, Move 37, was very strong, providing support to stones over a large swathe of the board. But, at the moment the move was made, it was impossible to trust by the human opponent because they could not evaluate the competency of the action based on the information available about its genesis. What was AlphaGo? How does it think? What grounds its decisions? How does it make its decisions? Human understanding is critical to trust between humans and AS. It is likely in the future that more and more AIs driving AS are complex, sophisticated intellects, born of machine learning and other architectures. The danger is that humans do not trust them because they cannot understand them.

Smithson in Sect. 9.7 discuses people's aversion to systems that conflict with their own forecasts and diagnoses. Users view autonomous systems as less trustworthy if they do not understand how they operate, for example, if users do not know all the possible failure modes of an autonomous system, they will trust it less than if they know these states. His argument supports the hypothesis here that people are most likely to trust systems that produce results aligned with human-levels of decision-making.

Consider if AlphaGo was a platoon commander, sending troops into a war zone. Imagine, just as in move 37, the AS commander ordered soldiers to go to a place they could not make sense of; that they felt put their lives or civilian lives at unnecessary risk? Keep in mind that each soldier has a duty to disobey an unlawful order if its illegality is immediately obvious, such as procedural irregularity or moral gravity [71]. In these cases, humans ought not trust the AI, even if the AI proves to be more competent than human decision makers. The AI could have access to huge repositories of data unable to be processed by humans. These calculations and decisions are frightening to humans and justify wariness and skepticism. Even more significantly, suppose complex sophisticated AIs were in charge of Lethal Autonomous Weapons Systems (LAWS), both decisions to target and decisions to fire, how do we know

whether to trust them? How would deaths be judged just or unjust if the algorithms deciding who dies are beyond human comprehension? LAWs led by AIs may lead to unintended initiation of armed conflicts and the unjust escalation of conflicts [5].

It is important to note that leading manufacturers of LAWs currently require human oversight and judgment for all decisions to target and to fire [5]. Current restrictions are based on the notion that humans are better decision-makers than machines. However, manufacturers continue to build incrementally autonomous capabilities across all systems. To imagine the impact of increasing autonomy for weapons systems, it is instructive to consider how other industries have rolled out autonomous systems and their impact on human users. Car manufacturer Tesla released a self-driving mode on its cars with the requirement that humans always have their hands at the wheel. Yet, Tesla drivers drive while deliberately disobeying protocols because they trust that the systems *do not* actually require their oversight [86]. There is evidence as AS become increasingly sophisticated humans may become either overly trusting or overly skeptical. Consider research on autonomous offshore oil drilling system operations [34]. Drill operators sometimes abandon their duty to oversee AS due to competing cognitive demands or they ignore the AS and make their own decisions inefficiently. In both cases the level of trust in the autonomous system plays a direct role in how humans view their obligations to participate in broader systems operations or obey oversight protocols. In sum, while there are currently policies requiring LAWs to be under ultimate human control, the pressures and stress of combat may lead to humans relinquishing control. In the future humans may not have the competence to be in control of these systems.

Perhaps more frightening is a future where AS knows how to manipulate consent and trust in humans [10]. This is a situation where we trust an AS because it is clever enough to manufacture our trust. But, it does so in either a disingenuous or manipulative way. It is not hard to imagine such an AI capitalizing on inductive trust tendencies or biases in humans. Consider Nelson Goodman's [32] thought experiment about the colour of emeralds known as the 'grue-paradox' [18]. In this hypothetical, all our experience of emeralds is their greenishness, so we ascribe to them the stable and persistent property 'green'. Goodman points out that in fact, Emeralds might be not green but 'grue'. Grue is a property of objects that makes them look green until a particular time (e.g. 2025), but look blue afterwards:

Definition 1 x is grue $=_{df}$ x is examined before t and green $\bigvee$ x is not so examined and blue.

If Emeralds are grue, they have never been green. Now suppose we take this hypothetical case of false induction (i.e. trying to establish facts about emeralds and their colour from history and experience) and consider malevolent programmers building an AS. These programmers design a robot that engenders trust over time, for a long time, like an embedded undercover operative. During production and deployment, the AS passes every test humans and regulators can design to establish its trustworthiness. The AS is tested in hundreds of real time situations and thousands of simulated scenarios. But, unbeknownst to regulators, it has been programmed to

switch modes in 2025 while deeply embedded in society. So, humans trusted it, but then the AS betrays them and carries out its secret objective. There was no way to know, inductively that the AS would flip. That it was actually an untrustworthy AS. It is also concerning to consider if such hidden higher-level objectives can be programmed, such programs could be activated or changed remotely and iteratively-threatening the integrity of the AS.

9.4.4 Trustworthiness and Risk

Finally, when ascribing trustworthiness to agent Y, X needs to consider the context of decisions. We have different thresholds for trust depending on the risk of the decisions that have to be made and this in turn depends on impact of decisions-see Fig. 9.3. This figure shows the relationship between decision impact, trustworthiness and trust. Life-threatening decisions, such as our choice of neurosurgeon have a higher threshold for trust than merely inconvenient decisions such as our choice of lawyer to settle a contract on a house. Consider PARO, a robot that resembles a baby-seal designed to assist the elderly similar to pet therapy. If PARO malfunctions, very little is lost to the humans who rely on it. But if a rescue robot malfunctions during an evacuation human lives are at stake. If 0 = no trust and 1.0 = absolute trust, We may need to trust our surgeon 0.99 in order to agree to brain surgery, but only need to trust our check out clerk 0.65 in order to complete our retail shopping. This is relevant in AS where similar algorithms may be installed or implemented into a

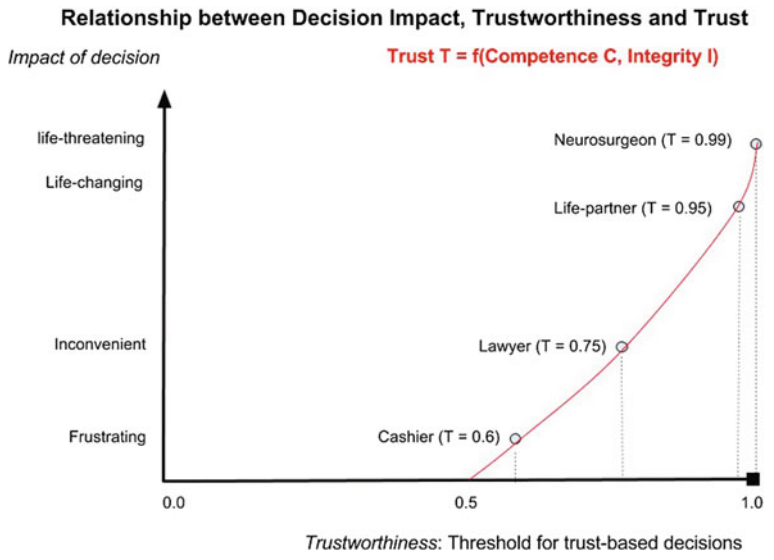

Fig. 9.3 Relationship between decision impact, trustworthiness and trust

huge variety of contexts. We can imagine perceptual and mechanical algorithms that allow a capsicum-picking robot [55] to drop 1 in 10 vegetables being reconfigured to help in a rescue operation where dropping 1 in 10 children from a boat is absolutely unacceptable.

9.4.5 Summary

This section examined the epistemology of trustworthiness. Implicit indicators of trust can be grounded in physical responses and intuitions as well as reputational features of the system that designed and built the AS. Explicit, reflective or rational trust can be elusive, but must stem from our experience of people over time and our reasons to judge their trustworthiness. As AS become more complex, reasons to trust need to be curated from teams of experts including regulators, designers, engineers, users and so forth. Inductive reasoning may need to be augmented by abductive reasoning for radically innovative AS that involve untested combinations of systems and/or new types of systems.

Even once explicit evaluation methods are established, the increasing competence of AS is a risk to human trust. I argue that increased competence increases trust in AS by humans both for implicit and explicit justifications up until competence far exceeds human comprehension. As AS competence continues to increase, humans may cease trusting them because they do not understand them (perhaps frustrating engineers and designers). Or, perhaps even worse, they falsely trust malevolent systems that should not be trusted. Either way, humans may become unreliable at evaluating trustworthiness as AS surpass human cognitive capacities.

9.5 What or Who Should We Trust?

What or who should we trust? Robots and AS should be programed with our best normative theories of logic, rationality [46] and ethics tempered with pragmatic performance expectations. Robots and AS are already computational devices, thus abide by propositional logic, predicate logic, and sometimes paraconsistent logic [93]. Robots increasingly make decisions under uncertainty using Bayesian rationality [8, 92]. In the future, robots and AS will be designed to test newer normative theories of rationality such as quantum cognition [13] (See Sect. 10). Ethically, we should trust humans and AS that take care of our interests and obey the law. This section will briefly survey ethical theories that AS ought to abide by.

Legal frameworks can do some of the normative heavy lifting for AS, but unfortunately the law is not nearly nuanced enough to cover human-judged ethical behaviours. For example, suppose a tree branch has fallen on the road during a storm [57]. A human driver would cross double-yellow lines on a road to go around the branch once a safety-check was undertaken and we would judge her ethical. How-

ever, for us to trust an autonomous car to make the same judgment, violating legal requirements regarding double-yellow lines, it would need to know a huge range of concepts and contexts, e.g. computational versions of terms such as 'obstruction' and 'safe' [31]. Humans make decisions that violate the law strictly speaking, but are usually nuanced actions that take context and risk into account.

In terms of human rights, AS ought to be aligned to the United Nations Declaration of Human Rights, the Geneva Conventions and Protocols [44]), and human rights law [6]. Additionally, AS ought consider a broad range of ethical theories from philosophy. Consequentialism (or 'Utilitarianism') is a dominant ethical theory that would justify AS actions if they cause the most happiness or 'utility'. For a Utilitarian, LAWs would be justified if they remove human error, thus reduce civilian casualities. Self-driving cars are justified if they massively reduce the road toll, even if the occasional person or bystander is killed through error. Utilitarian arguments are the most frequently cited arguments in favour of deploying autonomous systems. Deontological arguments focus not on the ends of decisions, but the way decisions are made, aka 'the ends do not justify the means'. Kant might agree that lying to all children about the existence of Santa creates the most happiness, but, it is unethical because it violates the Categorical Imperative [73]. A deontologically or 'duty' based AS may have a duty to retain all records of software upgrades and decision parameters in an impenetrable black box for later insurance claims and legal determinations regardless of whether such records end up disproportionately punishing low socioeconomic groups. Each design decision can be worked through from different ethical perspectives including social contract theory, virtue ethics or feminist ethics. While different theories may demand conflicting design decisions, many decisions may come out the same. For example, there are both Utilitarian and Kantian justifications for rescue robots to obey triage rules in a rescue. On the other hand, some ethical theories provide a unique way of understanding how and why we trust each other under stressful and uncertain circumstances. Virtue ethics justifies action not based on their consequences or intention, but on virtues such as bravery and honour. Where as Utilitarian or Kantian principles could possibly be coded into a decision maker, virtue is built up over time, via experience and feedback calibrating specific actions against virtuous norms. Virtue ethics could be incorporated into probabilistic decision systems because the right action is not the one that always produces the best outcome. Under virtue ethics we trust an AS if it made the best decision possible in its context given its operating parameters. Additionally, newer ethical theories might fill in some decision-making gaps. For example, Feminist ethics [45] could justify preferential care behaviours in a special operations team. There is a particular synchronicity between virtue ethics and feminist ethics that could be fruitful for building trust [35].

Our reliance on people and AS is affected by our level of dependence and cooperation. Our trust in our life partner to care for us involves a multi-faceted risk and trust over time (with shared cognition) versus the one-off trust we might place in a surgeon. For example, we don't really care if our surgeon is nice to his in-laws at Christmas, just so long as he can remove the tumour. We trust people who we believe have strong reasons for acting in our best interests [38]. The main incentive

for these reasons is a desire to maintain a strong relationship with us (whether that is economic, love, friendship etc.). Trust between individuals is different to trust we have in corporations. This asymmetry is a really significant issue for AS, because humans ground their trust in beliefs about the corporation behind the AS, not the systems themselves instantiated in a single car, robot, or computer installation. Social norming is an approach to procedural ethics outside of traditional philosophical theories from anthropology and sociology [101]. Social norming is about learning how to behave in groups to get along the best. It requires we understand social expectations. Detailed theories of cooperative behaviour stem from disciplines such as sociology, biology, anthropology and group psychology. These models are not about competence and achieving optimal performance on tasks, but about creating the most cohesive, resilient teams of organisms. Theories such as game theory contribute to understanding social norming [72]. One of the many advantages of group level norms is the ability to train AS with social norming without needing top-down ethical theories to drive behaviours.

However, while there are promising avenues for research into the ethical programming to improve trust, many barriers exist for the universalization of such programming. This is because there remains vast disagreement on what the right ethical principles are or even whether ethical principles exist such that they could be implemented into an AS. What does ethical talk amount to? It seems that humans judge each others actions as ethical or not ethical based a huge range of theoretical, contextual, pragmatic and social factors that ethical theories struggle to explain beyond stipulating that actual human decision makers exhibit a sort of hopeless contrariness.

There is a lot of work to be done in determining what the most ethical action is in any particular context and what model underpins such actions. However, even if we can program AS to be ultimately logical, rational or ethical, humans may be uncomfortable. Would we trust machines that obey norms without empathy [28]? Consider the origins of the word robot from the 1920 play, Rossumovi Univerzální Roboti (Rossum's Universal Robots). In the play Czech writer Karel Capek endowed robots with not just thoughts, but emotions to enable them to increase their productivity [97]. Capek's robots were forced workers more like biological androids Replicants in Bladerunner than metal machines. If we program AS with emotions and empathy to build trust, will they suffer if we treat them badly? If AS are moral agents that can suffer, then building trustworthy autonomous systems also means building an ethical and legal framework around their use and identifying their rights [81]. Japanese roboticists are already designing robots to have 'kokoro', translated into heart, spirit or mind [1]. Kokoro stems from animist spiritual thinking that all objects, including rocks and trees, have some level of consciousness and agency including emotions, intelligence and intention. Robots and AS of the future may need complex social identities to meet ethical and social norms.

9.6 The Value of Trustworthy Autonomous Systems

The discussion of the metaphysics, epistemology and normativity of trustworthiness has assumed that trustworthy AS are the desired goal. However, do humans want their decisions automated even if available AS are trustworthy? One the one hand optimising AS could be ideal for human-robot interactions, freeing up time and resources, but on the other hand, perhaps humans want to make their own decisions? We might think that humans develop a sense of identity and security from decision making responsibility in their roles and jobs and that we risk devaluing human workers by outsourcing decisions to AS. If so, then even if AS increase process productivity, it may decrease productivity overall. Alternatively, humans may find work tedious and be glad for near-optimal autonomous task allocations [30]. In the Culture novels by science fiction writer Iain M. Banks, the AS 'Minds' make most human decisions that aren't spiritual or fun and the human populace are perfectly content [79]. 'Minds' are sentient hyper-intelligent AIs on space ships and inhabited planets that have evolved to become far more intelligent than their original biological creators. The minds have taken over the administrative infrastructure of the Culture civilization. We don't have to go too far to see that humans already welcome efficiencies that stem from machine learning when they use their smart phones. How many decisions and what sorts of decisions will humans outsource to an AS if given the opportunity?

Interestingly Gombolay et al. [30] found that contrary to their hypotheses (and in alignment to Iain M. Banks), humans prefer to outsource decision making to autonomous robots even when they perceived their human co-leader more favorably than their robotic co-leader. Interestingly, in follow up questionnaires, subjects felt that their human co-leader had additional properties, such that they liked, appreciated and understood them, that humans understood, trusted and respected each other, and finally that subjects and human co-leaders were important to the task. However, liking humans and wanting them around is not the same as wanting humans to make decisions.

One of the important distinctions when considering AS is the difference between physically instantiated AI (e.g. personal robot) that learns and grows with an individual or team, versus an integrated AI programmed to act over many physical bodies (e.g. networked self-driving cars) that show no preferential or focused behaviours with individual humans. In the latter case, Iain M. Banks Minds and Apple's subtle machine learning might work fine. But, in the former case, social norming may be the right solution.

9.7 Conclusion

This chapter has examined the trustworthiness of autonomous systems. I have argued that effective robots and autonomous systems must be trustworthy and the risks of reliance justified relative to perceived benefits. Trustworthiness is a dispositional and

relational property of agents relative to other agents within spatiotemporal bounds. Trustworthy agents must be reliable (incorporating adaptability and redundancy). A two-component model of trust was used to differentiate factors of competence (skills, reliability and experience) to factors of integrity (motives, honesty and character). When humans evaluate the trustworthiness of autonomous systems and other humans they use intrinsic, 'gut' level cues such as physicality as well as extrinsic 'top down' reasoning. Humans tend to trust agents operating within the bounds of human cognition and are less trusting as systems operate at super-human levels. The threshold for trustworthiness of an agent or organisation depends on the impact of decisions in a particular context. Building trustworthy autonomous systems requires obeying the norms of logic, rationality and ethics under pragmatic constraints-even though there is disagreement on these principles by experts. AS may need sophisticated social identities including empathy and reputational concerns to build human-like trust relationships. Ultimately transdisciplinary research drawing on metaphysical, epistemological and normative human and machine theories of trust are needed to design trustworthy autonomous systems for adoption.

References

1. S. Šabanović, Inventing Japan's 'robotics culture': the repeated assembly of science, technology, and culture in social robotics. Soc. Stud. Sci. **44**(3), 342–367 (2014)
2. D. Adams, *The Hitchhikers Guide to the Galaxy* (Pan Books, UK, 1979)
3. J.R. Anderson, *How can the Mind Exist in a Physical Universe* (Oxford University Press, Oxford, 2007)
4. K.J. Arrow, *The Limits of Organization, Fels Lectures on Public Policy Analysis* (W. W. Norton and Co., New York, 1974)
5. P. Asaro, Killer robots and the ethics of autonomous weapons, in *Ethics of Artificial Intelligence., NYU*, 14–15 Oct 2016
6. P. Asaro, On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making. Int. Rev. Red Cross **94**(886), 687–709 (2012)
7. I. Basterretxea-Iribar, I. Sotés, Jose Ignacio Uriarte, Towards an improvement of magnetic compass accuracy and adjustment. J. Navig. **69**(6), 1325–1340 (2016)
8. P. Bessière, C. Laugier, R. Siegwart, *Probabilistic Reasoning and Decision Making in Sensory-Motor Systems*, vol. 46 of *Springer Tracts in Advanced Robotics* (Springer Science & Business Media, 2008)
9. Boston Dynamics, Introducing spot, https://youtu.be/M8YjvHYbZ9w. Retrieved from 9 Feb 2015
10. N. Bostrom, Ethics of artificial intelligence, in *Ethics of Artificial Intelligence, NYU*, 14–15 Oct 2016
11. C. Breazeal, M. Siegel, M. Berlin, J. Gray, R. Grupen, P. Deegan, J. Weber, K. Narendran,break J. McBean, Mobile, dexterous, social robots for mobile manipulation and human-robot interaction, in *ACM SIGGRAPH 2008 new tech demos* (ACM, 2008), p. 27
12. C.L. Breazeal, *Designing Sociable Robots* (MIT Press, Cambridge, MA, 2002)
13. J.R. Busemeyer, P.D. Bruza, *Quantum Models of Cognition and Decision* (Cambridge University Press, Cambridge, 2012)

14. J. Butler, P. Giuliano, L. Guiso, *The right amount of trust* (Electronic book section, National Bureau of Economic Research, 2009)
15. J.R. Carbonell, AI in CAI: an artificial-intelligence approach to computer-assisted instruction. IEEE Trans. Man Mach. Syst. **11**(4), 190–202 (1970)
16. N. Carl, F.C. Billari, Generalized trust and intelligence in the United States. PLOS ONE **9**(3), e91786 (2014)
17. D. Chen, G. Chang, D. Sun, J. Li, J. Jia, X. Wang, TRM-IoT: a trust management model based on fuzzy reputation for internet of things. Comput. Sci. Inf. Syst. **8**(4), 1207–1228 (2011)
18. D. Cohnitz, M. Rossberg, Nelson goodman, in *The Stanford Encyclopedia of Philosophy*, ed. by E.N. Zalta (Stanford Encyclopedia, 2016)
19. B.L. Connelly, T.R. Crook, J.G. Combs, D.J. Ketchen, H. Aguinis, Competence- and integrity-based trust in interorganizational relationships: Which matters more? J. Manage. (2015)
20. B.L. Connelly, T. Miller, C.E. Devers, Under a cloud of suspicion: trust, distrust, and their interactive effect in interorganizational contracting. Strat. Manage. J. **33**(7), 820–833 (2012)
21. L. Cosmides, H. Clark Barrett, J. Tooby, Clark Barrett, and John Tooby. Adaptive specializations, social exchange, and the evolution of human intelligence. Proc. Natl. Acad. Sci. U.S.A. **107**(Supplement 2), 9007–9014 (2010)
22. J. Downer, *When failure is an option: redundancy, reliability and regulation in complex technical systems* (Economic and Social Research Council, Government document, Centre for Analysis of Risk and Regulation, 2009)
23. J.B.M. Engelman, *An empirical investigation of the evolutionary and ontogenic roots of trust*. Thesis, 2014
24. P. Faulkner, On telling and trusting. Mind **116**(464), 875–902 (2007)
25. P. Faulkner, *Knowledge on Trust* (Oxford University Press, Oxford, 2011)
26. G. Flanagan, If you think Apple is a cult, you haven't been to a Tesla event, in *Business Insider*, 14 Oct 2015
27. T. Fraichard, J.J. Kuffner, Guaranteeing motion safety for robots. Auton. Robots **32**(3), 173–175 (2012)
28. E. Gleichgerrcht, L. Young, Low levels of empathic concern predict utilitarian moral judgment. PloS one **8**(4), e60418 (2013)
29. A. Goldman, Epistemology and the evidential status of introspective reports. J. Conscious. Stud. **11**(7–8), 1–16 (2004)
30. M.C. Gombolay, R.A. Gutierrez, S.G. Clarke, G.F. Sturla, J.A. Shah, Decision-making authority, team efficiency and human worker satisfaction in mixed human-robot teams. Auton. Robots **39**(3), 293–312 (2015)
31. N.J. Goodall, *Machine Ethics and Automated Vehicles* (Springer, DE, 2014)
32. N. Goodman, *Fact, Fiction, and Forecast* (Harvard University Press, Cambridge, 1983)
33. M. Granovetter, Economic action and social structure: the problem of embeddedness. Am. J. Sociol. **91**(3), 481–510 (1985)
34. L.J. Gressgård, K. Hansen, F. Iversen, Automation systems and work process safety: assessing the significance of human and organizational factors in offshore drilling automation'. J. Inf. Technol. Manage. **24**(2), 47 (2013)
35. R. Halwani, Care ethics and virtue ethics. Hypatia **18**(3), 161–192 (2003)
36. P.A. Hancock, Imposing limits on autonomous systems. Ergonomics **60**(2), 284–291 (2017)
37. P.A. Hancock, D.R. Billings, K.E. Schaefer, Can you trust your robot? Ergonomics Des.: Q. Hum. Factors Appl. **19**(3), 24–29 (2011)
38. R. Hardin, *Trust and Trustworthiness* (Russell Sage Foundation, New York, 2002)
39. K. Hawley, Trust, distrust and commitment. Noûs **48**(1), 1–20 (2014)
40. P. Hieronymi, The reasons of trust. Australas. J. Philos. **86**(2), 213–236 (2008)
41. E.S. Hinchman, Telling as inviting to trust. Philos. Phenomenol. Res. **70**(3), 562–587 (2005)
42. R. Hughes, Sensors for coastal remote sensing. Paper presented at the SpaceNet Remote Coastal Workshop, July 2015
43. D. Hume, *A Treatise of Human Nature: Being an Attempt to Introduce the Experimental Method of Reasoning Into Moral Subjects*. ebooks@Adelaide (1739)

44. International Committee of the Red Cross, Geneva conventions of 1949 and additional protocols, and their commentaries, 1949
45. A.M. Jagger, *Feminist Ethics* (Gardland Press, New York, 1992)
46. P.N. Johnson-Laird, R.M.J. Byrne, Models and deductive rationality, in *Rationality: Psychological and Philosophical Perspectives*ed. by K. Manktelow, D. Over (Routledge, London, 1993)
47. K. Kaneko, K. Harada, F. Kanehiro, G. Miyamori, K. Akachi, Humanoid robot HRP-3, In *2008 IEEE/RSJ International Conference on Intelligent Robots and Systems* (IEEE, 2008), pp. 2471–2478
48. A. Keren, Trust and belief: a preemptive reasons account. Synth. Int. J. Epistemol. Methodol. Philos. Sci. **191**(12), 2593–2615 (2014)
49. S. Khemlani, A. Harrison, G. Trafton, An embodied architecture for thinking and reasoning about time, in *The 38th Annual Meeting of the Cognitive Science Society, Philadelphia* (2016)
50. J. Kim, A. Alspach, K. Yamane, 3D printed soft skin for safe human-robot interaction, in *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)* (IEEE, 2015), pp. 2419–2425
51. P.H. Kim, D.L. Ferrin, D. Cooper, K.T. Dirks, Removing the shadow of suspicion: the effects of apology versus denial for repairing competence- versus integrity-based trust violations. J. Appl. Psychol. **89**(1), 104–118 (2004)
52. A.K. Kozlovic, Technophobic themes in pre-1990 computer films. Sci. Cult. **12**(3), 341–373 (2003)
53. S. Kubrick, A.C. Clark, 2001: A space odyssey [film] (1968)
54. J.D. Lee, K.A. See, Trust in automation: designing for appropriate reliance. Hum. Factors J. Hum. Factors Ergon. Soc. **46**(1), 50–80 (2004)
55. C. Lehnert, I. Sa, C. McCool, B. Upcroft, T. Perez, Sweet pepper pose detection and grasping for automated crop harvesting, in *2016 IEEE International Conference on Robotics and Automation (ICRA)* (2016), pp. 2428–2434
56. S. Levy, The iBrain is here and its already inside your phone: an exclusive inside look at how artificial intelligence and machine learning work at apple. back channel, 25 Aug 2016
57. P. Lin, The ethics of autonomous cars. *The Atlantic*, 8 (2013)
58. T. Lopez, Army changing basic training this October. Army News Service, 24 Sept 2015
59. Y. Luo, Contract, cooperation, and performance in international joint ventures. Strat. Manage. J. **23**(10), 903–919 (2002)
60. F. Maleki, Z. Farhoudi, Making humanoid robots more acceptable based on the study of robot characters in animation. IAES Int. J. Robot. Autom. **4**(1), 63–72 (2015)
61. S. Mattie, WALL-E on the problem of technology. Perspect. Polit. Sci. **43**(1), 12–20 (2014)
62. D.J. McAllister, Affect-and cognition-based trust as foundations for interpersonal cooperation in organizations. Acad. Manage. J. **38**(1), 24–59 (1995)
63. V. McGeer, Trust, hope and empowerment. Australas. J. Philos. **86**(2), 237–254 (2008)
64. C. McLeod, Trust, *The Stanford Encyclopedia of Philosophy*, electronic book section Trust, in ed. by E.N. Zalta (Stanford Encyclopedia, 2015)
65. C. Metz, In two moves, alphago and lee sedol redefined the future. WIRED.com, 16 Mar 2016
66. M. Mori, K.F. MacDorman, N. Kageki, The uncanny valley [from the field]. IEEE Robot. Autom. Mag. **19**(2), 98–100 (2012)
67. D. Naiditch, The meaning of life. Skeptics Soc. Skeptic Mag. **8**, 74 (2000)
68. G. Nave, C. Camerer, M. McCullough, Does oxytocin increase trust in humans? A critical review of research. Perspect. Psychol. Sci. **10**(6), 772–789 (2015)
69. A. Nguyen, J. Yosinski, J. Clune, Deep neural networks are easily fooled: high confidence predictions for unrecognizable images, in *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (IEEE, 2015), pp. 427–436
70. D.C. North, *Institutions, Institutional Change, and Economic Performance* (Cambridge University Press, Cambridge, 1990)
71. M.J. Osiel, Obeying orders: Atrocity, military discipline, and the law of war. *California Law Review* (1998), pp. 939–1129

72. E. Ostrom, Collective action and the evolution of social norms. J. Nat. Resour. Policy Res. **6**(4), 235–252 (2014)
73. H.J. Paton, *The Categorical Imperative: A Study in Kant's Moral Philosophy. Book* (University of Pennsylvania Press, Philadelphia, 1971)
74. Z. Pylyshyn, *Seeing and Visualizing: It's Not What You Think* (The MIT Press, Cambridge, MA, 2003)
75. T. Reid, *An Inquiry into the Human Mind: On the Principles of Common Sense* (Penn State University, 2000, 1764)
76. C. Reilly, Australia's first autonomous bus trial goes off without a hitch (or a driver). CNET, 1 Sept 2016
77. J.B. Rotter, A new scale for the measurement of interpersonal trust. J. Pers. **35**(4), 651–665 (1967)
78. D.M. Rousseau, S.B. Sitkin, R.S. Burt, C. Camerer, Not so different after all: a cross-discipline view of trust. Acad. Manage. Rev. **23**(3), 393–404 (1998)
79. Y. Rumpala, Artificial intelligences and political organization: an exploration based on the science fiction work of Iain M. Banks. Technol. Soc. **34**(1), 23–32 (2012)
80. K.E. Schaefer, J.Y.C. Chen, J.L. Szalma, P.A. Hancock, A meta-analysis of factors influencing the development of trust in automation: implications for understanding autonomy in future systems. Hum. Factors **58**(3), 377–400 (2016)
81. E. Schwitzgebel, M. Garza, A defense of the rights of artificial intelligences. Midwest Stud. Philos. **39**(1), 98–119 (2015)
82. C. Sganzerla, C. Seixas, A. Conti, Disruptive innovation in digital mining. Proc. Eng. **138**, 64–71 (2016)
83. S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, Security, privacy and trust in internet of things: the road ahead. Comput. Netw. **76**, 146–164 (2015)
84. E. Simpson, Reasonable trust. Eur. J. Philos. **21**(3), 402–423 (2013)
85. J.R. Sklaroff, Redundancy management technique for space shuttle computers. IBM J. Res. Dev. **20**(1), 20–28 (1976)
86. Slow News Day (Producer), Tesla's model S autopilot is amazing! (2016)
87. A. Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations. Book 4, Chap. 2.* (David Campbell Publishers, London, 1991 edn, 1776)
88. A. Srinivasan, J. Teitelbaum, J. Wu, DRBTS: Distributed reputation-based beacon trust system. In *2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing*, 29 Sept–1 Oct 2006, pp. 277–283
89. K. Sterelny, *The Evolved Apprentice* (MIT Press, Cambridge, 2012)
90. N. Steinfeld, "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. Comput. Hum. Behav. **55**, 992–1000 (2016)
91. The Tesla Team. A tragic loss (2016)
92. S. Thrun, D. Fox, W. Burgard, F. Dellaert, Robust monte carlo localization for mobile robots. Artif. Intell. **128**(1–2), 99–141 (2001)
93. C.R. Torres, J.M. Abe, G. Lambert-Torres, J.I. da Silva Filho, Paraconsistent autonomous mobile robot Emmy III, in *Advances in Technological Applications of Logical and Intelligent Systems: Selected Papers from the Sixth Congress on Logic Applied to Technology*, vol. 186 (IOS Press, 2009), p. 236
94. G. Trafton, L. Hiatt, A. Harrison, F. Tamborello, S. Khemlani, A. Schultz, Act-r/e: an embodied cognitive architecture for human-robot interaction. J. Hum. Robot Interact. **2**(1), 30–55 (2013)
95. S. Turkle, Authenticity in the age of digital companions. Interact. Stud. **8**(3), 501–517 (2007)
96. T.R. Tyler, *Why People Obey the Law* (Princeton University Press, Princeton, 2006)
97. M.K. Vukobratovic, When were active exoskeletons actually born? Int. J. Humanoid Rob. **4**(03), 459–486 (2007)
98. M. Wehner, R.L. Truby, D.J. Fitzgerald, B. Mosadegh, G.M. Whitesides, J.A. Lewis, R.J. Wood, An integrated design and fabrication strategy for entirely soft, autonomous robots. Nature **536**(7617), 451–455 (2016)

99. O.E. Williamson, Calculativeness, trust, and economic organization. J. Law Econ. **36**(1), 453–486 (1993)
100. WIRED.com (Producer), How tesla's self-driving autopilot actually works, 09 2016
101. D.H. Wrong, The oversocialized conception of man in modern sociology. Am. Sociol. Rev. **26**, 183–193 (1961)
102. T. Yamagishi, *Trust as a form of social intelligence* (Russell Sage Foundation, New York, 2001)
103. T. Yamagishi, *Trust: The Evolutionary Game of Mind and Society* (Springer, Berlin, 2011)
104. Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for internet of things. J. Netw. Comput. Appl. **42**, 120–134 (2014)
105. H.A. Yanco, A. Norton, W. Ober, D. Shane, A. Skinner, J. Vice, Analysis of human-robot interaction at the DARPA robotics challenge trials. J. Field Robot. **32**(3), 420–444 (2015)