Volume 4, No. 6 | November–December 2021

RAIL
The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL The Journal of Robotics, Artificial Intelligence & Law
Volume 4, No. 6 | November–December 2021

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. Copyright 2021 Fastcase, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Journal Designer: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

Defining Autonomy in the Context of Tort Liability: Is Machine Learning Indicative of Robotic Responsibility? Part II

Katherine D. Sheriff*

Bypassing the issue of legal personhood, this article focuses on whether machine learning heightens robotic accountability and asks if the law should hold robots liable because a harm-creating decision was not a function of software programming but of robotic choice. It then recommends a variation of Ugo Pagallo's "digital peculium" liability scheme for "hard cases" involving robotic decisions absent appropriate linkage to the original programmer. It concludes by situating "hard cases" outside the scope of pre-programmed uncertainty within the larger abstraction laid out by HLA Hart and Ronald Dworkin, considering whether determination of a right answer, or conclusive indetermination of any, exists for application of legal accountability to ever-increasing robotic autonomy.

The first part of this article outlined traditional notions of learning and brain activity juxtaposed against software-engineered machine learning. It then described the existing scholarly debate surrounding the issue of robotic autonomy and explains how this debate impacts the applicability of tort liability to robots.

This part argues that because situations exist that cannot be pre-programmed, there is a strong case for mandated insurance carried by all robots to protect injured victims in those situations where fully autonomous machines "choose" a course of action too far removed from the work of the original programmer.

Then, this article recommends a variation of Ugo Pagallo's "digital peculium" liability scheme to account for the situations just described, where fully autonomous robots make decisions absent the appropriate linkage to the original creator and outside the scope of the uncertainty already programmed.

Finally, this article concludes by looking first to the allocation of systemic risk as a matter of organizational psychology and second the location of the hard case discussed in this article in the larger abstraction laid out by Ugo Pagallo and HLA Hart and

Robotics, Artificial Intelligence & Law / November–December 2021, Vol. 4, No. 6, pp. 403–421.

ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

Ronald Dworkin before him—the determination of a right answer or conclusive indetermination of any answer to robotic application queries.

Argument: Beyond the Digital Peculium

Liability model proposals range from registering autonomous robots as corporations to equipping each machine with its own insurance.[77] In *Cognitive Automata and the Law*, Giovanni Sartor explains, "One can only predict the [behavior] of the chess-playing system by attributing to it goals (winning the match, attacking a certain piece, getting to a certain position), information (about what moves are available to its adversary), and assuming that it can devise rational ways to achieve those goals according to the information it has."[78]

To explain machine learning, a few examples are useful to distinguish popular perception from the reality of current technological capabilities:

- Fuzzy driving;
- Robot erasing its own hard drive; and
- Third-party hackers commandeering a test drive.

First, practitioners generally agree that at least currently there is much human acting and, therefore, responsibility in play. To implement "fuzzy driving"—or any software program—would require parameters of some sort at the outset.

One example is a program determining an autonomous vehicle's actions at a four-way stop. Commands might include how many vehicles to let pass via that jurisdiction's traffic rules, a time limit to sit and wait before attempting to go ahead, or how aggressively to behave upon going through the intersection. For instance, commands could vary from "floor it" in the most aggressive sense to nudge-and-creep in a more passive approach.[79]

Similarly, autonomous vehicle software commands go to vehicle spacing on the highway or major public roads. If the jurisdiction requires drivers to always maintain a minimum distance of two vehicle lengths, then for the autonomous vehicle to learn this rule, some human programmer had to set how to learn the rule.[80]

Finally, an analogy to defensive driving is instructive: Think of a parent teaching their super-intelligent, but completely inexperienced, teenager to drive. The lesson of the day is avoiding merging vehicles that might dangerously "cut off" the teenager's vehicle on the highway.

A more cautious parent might instruct the teenager to shift over one lane or drop back to allow the imposing vehicle to merge in a safer manner. Another parent might suggest more aggressive maneuvers like cutting down the space between vehicles, honking or other attention-getting, mildly assertive actions to deter other vehicles from merging.[81]

To explore the second example, consider the robot that erases its own hard drive. Many practitioners lament the "Hollywood-esque" depiction of independent action by autonomous vehicles as far-fetched. Perhaps the computer "driving" the vehicle is a complete operating system in itself and the navigation software user has some sort of access permissions or awareness of how to run the programs to erase the data. Navigation software user means any piece of software running an operating system, which usually must be signed into with either a user identification number or other account number—even if the ID or account is a dummy service or a system account doing maintenance.[82]

Arguably, if this were the case, there would—or at least could—be some configuration for a logfile originally generated by actions that the service account performed, provided the logfile was not otherwise disabled or deleted.[83] Essentially, unless the impact of a crash physically damaged the hard drive via electromagnetic pulse, it is difficult to conceive of a way the erasure is possible absent some human putting the program on the computer with directions to erase first.[84]

Finally, the third example involves third-party hackers commandeering a vehicle test drive. The fear that hackers might sabotage the autonomous vehicles market by interfering with the vehicle's functioning has been the subject of mainstream news. A vehicle manufacturer with onboard computers had a service account left open or unlocked. Hackers discovered the security gap and took advantage by toying with drivers of the vehicles by turning on the radio and even killing the ignition.[85]

Importantly, product design must be understood as a tool with a specific purpose. In *What Is a Designer*, Norman Potter emphasizes the importance of distinguishing between different forms of design and identifies three methods for conceiving the notion of design: environmental design of spaces, product design of objects, and communication design of messages.[86]

Further, there are three subjects of design: places, products, and organisms.[87]

In this context, Pagallo explains it is impossible to program software to prevent forms of harm-generating behavior because such "constraints emphasize critical facets of design underlying the use of allegedly perfect self-enforcing technologies."[88]

Discussing the role of design in robotics law, Pagallo explains: "In addition to projects encouraging agents to change their conduct (e.g., speed bumps), or decrease the impact of harm-generating behavior (e.g., air bags), think of design for AI cars, which should be able to stop or limit their speed according to the inputs of the surrounding environment."[89]

Further, "preventing harm-generating conduct from even occurring impacts on the security of the robotic system through the use of driver checking mechanisms and cruise control, blind spot monitoring and traffic sign recognition, pre-crash schemes and so forth."[90] Thus, "[s]uch systems will increasingly be connected to a networked repository on the internet that allows robots to share the information required for object recognition, navigation and task completion in the real world."[91]

Pagallo concludes: "The environment of AI car behavior is thus designed as a complex multi-agent system where maintenance and safety contractors, traffic operators and internet controllers, interact with autonomous or semi-autonomous machines in order to avoid collisions, communication interferences, environmental concerns, and more."[92]

So, in the fuzzy driving, hard drive erasing, and test drive hacking examples, "sweeping generalizations hardly fit the law of robots" because while some high-stakes robotic applications "truly challenge basic pillars of the law," this is not so in other applications such as service robots.[93]

Accordingly, one strategy has been introducing the public to plain cases of the laws of robots so as to distinguish these cases of general agreement from "the *hard cases* induced by increasingly autonomous robots."[94] General agreement exists as to how to treat:

- Responsibility pursuant to the liability model in accomplice cases within criminal law;

- Responsibility that depends on the voluntary agreement between private persons in the civil law field; and
- Strict liability for dangerous activities in tort law.[95]

Pagallo explains this distinction between easy and hard cases: "In all of these [easy] cases, there is no such thing as a failure of legal causation that suggests bringing robots back under human control."[96]

The Impact of Liability for Robotic Decision Making

In ancient Rome, forms of responsibility stemmed from "the general idea that individuals are liable for unlawful or accidental damages caused to others due to personal fault."[97] In hard cases, Pagallo expects increasing robotic autonomy. The issue beyond the reach of this discussion remains, that is, how to assign novel kinds of liability for another's behavior. Pagallo explains, "For the first time ever, legal systems will hold humans responsible for what an artificial state-transition system 'decides' to do."[98]

Such robotic liability "crucially depends" on the different kinds of robots used (nanny, robot toy, robot chauffeur, robot employee, etc.). Perhaps some of the most innovative aspects in the field of the laws of robots are new strict liability policies like that suggested by Richard Posner. Strict liability policies have been considered complementary to traditional forms of responsibility for the behavior of children, pets, or employees.[99]

Alternatively, children, pets or domestic animals, and employees might be accounted for through mitigating insurance models, authentication systems, or varying allocations of the burden of proof.[100]

Systemic Risk and Organizational Psychology: The Economic Impact

Systemic risk in legal systems, as described by J.B. Ruhl, proposes that legal systems survive when sufficiently robust.[101] To be sufficiently robust, then, a legal system must be:

- Reliable;
- Efficient;
- Scalable;
- Modular; and
- Evolvable.[102]

Regardless of the level at which a legal system is representative of functionality traits, "even with no other causal force in play, the architecture of legal systems necessarily embeds some degree of systemic risk in the system's behavior. [It is] the architectural design that matters as to how much [risk is embedded in the system]."[103]

Systems engineers David Anderson and John C. Doyle devised the "robust yet fragile" dilemma to bring to light the "inherent quality of any complex adaptive system."[104] As Anderson and Doyle explain:

> Historically, we have done a poor job in managing the fragilities created by our complex networks, from global warming to ecosystem destruction, global financial crises, etc. In many cases, past failure are due to fragilities that were direct side effects of mechanism that promised to provide great benefits, including robustness. We are much better at designing, mass-producing, and deploying network-enabled devices than we are at being able to predict or control their collective behavior once deployed in the real world. The result is that, when things fail, they often do so cryptically and catastrophically.[105]

Similarly, vulnerability theory as explicated in Martha Fineman's Vulnerability Thesis, posits that there is a certain resilience necessary for legal systems to function optimally.[106]

Fineman discusses reallocation of responsibility in state and market institutions as a collective burden ideally borne by society as a vulnerable whole.[107] A "responsive state" recognizes institutional responsibility for all legal entities it brings into being through which individuals acquire and amass resources and the resilience necessary to confront the reality of vulnerability.[108] As a heuristic device, vulnerability can force examination of assumptions and biases within legal practices, including liability apportionment.[109]

Fineman and Grear explain:

> Resilience is not something we are born with. It is produced over time within social structures and under societal

> conditions over which individuals may have little control. This fact alone demonstrates that individual failure or success must be understood in terms broader than just individual responsibility. Success and failure are socially structured and intricately dependent on an individual's interactions within the institutions and political structures society has constructed.[110]

At base, "this fact of primary and inevitable dependence on societal institutions is true whether those institutions are deemed public or private or are labeled as 'family,' 'market' or 'state' entities."[111] Vulnerability theory, then, can be thought of as a means of determining what constitutes "ethical legislative behavior."[112]

Echoed elsewhere, the legal system must evolve: "Robot systems must evolve as well, and legal scholars have for centuries devoted attention to assessing how and why they do."[113] At base, "[a]ny legal system, if it is going to be effective, has to be able to evolve incrementally through practice."[114]

Ruhl gives the example of common law nuisance and the shared understanding that "changed circumstances or new knowledge may make what was previously permissible no longer so."[115] Considering the precautionary principle in the context of regulatory design, the "coevolution" of the regulatory system and the regulatory problem or "system of systems" highlights the systemic risk inherent in case-by-case failure assessments.[116] Burton and Egan's Interdependent Systems Analysis is the study through which such systems analysis erupted into the legal scene.[117]

Because the field of service robotics requires hardware to work in the physical world, developing robots is challenging in a way that other AI manifestations are not as yet. While robots operate easily in a controlled environment, release into the physical world amid the complex and often unpredictable situations creates uncertainty for robotic performance. AI and autonomous robots adorned with sensors and effectors unseen a decade ago provide a formidable challenger to the reigning champion that is the physical world in all its unpredictable splendor.[118]

Easy Cases, Hard Cases, and How to Deal: The Doctrinal Impact

According to Pagallo, analyzing varying layers of complexity "invoked" by the impact of robotic technology on the law can be presented via a summary of legal observations.[119] Pagallo's theme resonating throughout his work is that the intricacy of the analysis begets the complexity of the model.

The complex model may then be enhanced by layering fields of legal study, chiefly of robotic crimes, contracts, and torts. Pagallo's examples also include administrative law and the legal responsibility of regulatory authorities, such as those granting certificates to civil drones.[120] However, the greatest challenge presented in this article is defining critical terms.

Pagallo charged himself with the same goal to the end that "observables suffice to distinguish plain from hard cases in which the applicability of classifying terms sparks general disagreement."[121]

Examples Pagallo provides here occur in some clauses of criminal immunity and negligence in criminal law and torts.[122] Unreasonable conduct of robotic agents in tort law and accountability "robo-traders" for businesses and agreements in contracts round out Pagallo's examples of hard cases.[123]

At this grander level of abstraction, scholars compete to present the most persuasive explanation of, and proscription for, hard cases.

One group of scholars, as explained by HLA Hart in *The Concept of Law*, "reckon" that "there is no possibility of treating the question raised by the various cases as if there were one uniquely correct answer to be found, as distinct from an answer which is a reasonable compromise between many conflicting interests."[124]

The other oft-recognized group of scholars, led predominantly by Ronald Dworkin, propose solutions placing the principles of the legal system at the crux of analysis, "conceived as normative statements with a deontological, rather than teleological, meaning."[125] By following the "logic of yes or no, or what is good for all," Dworkin claims that a "right answer" can be found for every case.[126]

According to Dworkin, jurists "should identify the principles of the system that fit with the established law, so as to apply such principles in a way that interprets the case in the best possible light."[127] As Dworkin states in *A Matter of Principle*, this effort emphasizes the parallel between law and literature.[128] Dworkin writes that one "must read through what other judges in the past have written not only to discover what these judges have said, or their state of mind when they said it, but to reach an opinion about what these judges have collectively done, in the way that each of our novelists formed an opinion about the collective novel so far written."[129] In *Justice in Robes*, Dworkin explains that his opponents have not swayed his stance: "some critics, including Brian Barry and Joseph Raz, suggest that I have changed my mind about the character and importance of the one-right-answer claim, for better or for worse, I have not."[130]

Circumstances in which there is general disagreement depends on the fact that there are many right answers out there. Analogy and principled legal reasoning at times provide unequivocal solutions but a number of issues often remains open as in:

- Criminal negligence cases;
- Agenthood issues in contract law; and
- Policy debates of tort law.[131]

Taking tort law, for example, policy answers vary across different traditions, customs, and legal cultures, as is apparent in Pagallo's comparison between the American (forms of negligence-based accountability) and Italian (traditional policies of no-fault responsibility) models in the field of tort liability.[132]

In *Law's Empire*, Dworkin suggests that "[f]or every route that Hercules took from that general conception to a particular verdict, another lawyer or judge who began in the same conception would find a different route and end in a different place, as several of the judges in our sample cases did. He would end differently because he would take leave of Hercules, following his own lights, at some branching point sooner or later in the argument."[133]

Yet Pagallo reminds his reader that there is still another set of cases in which general disagreement depends more on different moral and political assumptions than technicalities of legal expertise.[134]

For example, Christof Heyns recommended Secretary-General Ban Ki-moon commission experts to tackle "the fundamental question of whether lethal force should ever be permitted to be fully automated" in his capacity as Special Rapporteur on extrajudicial executions.[135]

Consider then whether a certain type of drone design should be considered legal in the field of robotics military technology. Further, consider what should be the design of the new environment of such human-robot interaction. Taking a step back, consider whether "a reasonable compromise on the basis of legal expertise, rather than the search for any right answer, is at stake."[136]

One view is that the intricacy of this system makes probable a failure of legal causation.[137] To some, the best method of accident or risk control is to scale back activity through strict liability policies.[138] Other opinions center on the claim that social and technical transactions run by artificial agents should be brought back under human control.[139]

Value judgments made in Pagallo's analysis involve two distinct steps. Echoed in current debate, Pagallo stresses the normative question, that is, which hard cases should have priority:

- Robot soldiers;
- Accountability of robots in contracts;
- New mechanisms of personal accountability for robots and clauses of negligence-based responsibility extended to the field of torts; and
- The use of robots as innocent means of human *mens rea* or guilty mind.[140]

In every hard case, "[s]elf-enforcing technologies would prevent robotic behavior and might impinge on individual freedoms by unilaterally determining how the artificial agents should act when collecting the information."[141]

Conclusion: Expanding the Level of Abstraction for a Better View

Tort law exists to hold accountable those responsible for accidents, to encourage all actors to be more careful, and, ultimately, to make injured victims whole. The noted tension in academic debate looks at how traditional notions of responsibility and personhood comport with the advent of AI in its many forms. The role that notions of traditional learning patterns and brain functionality play in the changing landscape of service products incorporating AI, now available for everyday use, is being both underestimated and underutilized.

Machine learning, though widely studied, has not been given due weight in considerations of liability in traditional negligence cases. Using current neuroimaging and organizational psychology, this article argued that decision making does not occur as traditionally portrayed. The brain is not an ideal analogue for machine learning.

The limits of the current legal framework would benefit from institutional recognition of current AI technology operating within tort liability. In the legal framework for tort liability, problems are occurring primarily in liability determinations and apportionment.

Further research should address such challenges of this field—as first coined by Asimov in the early 1940s: "robotics."[142]

According to Isaac Asimov's 1950 science fiction work, *I, Robot*, the three laws of robotics are as follows:

1. A robot may not injure a human being or through inaction allow a human being to come to harm.
2. A robot must obey the orders given to it by human beings except where such orders would conflict with the first law.
3. A robot must protect its own existence as long as such protection does not conflict with the first or second law.[143]

"More than 70 years later, it is remarkable how his plots foresee many of the crucial issues of today's debate: the legal personhood of robots, questions of logic on how the 'laws of the law' have to be interpreted, design of machines that should comprehend and process such sophisticated info as the current laws (of war and 'rules of engagement')."[144]

In fact, Asimov's message seems to hold, and Pagallo agrees, that robots are here to stay the societal and legal ought to be prudent governance recognizing the new "mutual relationships."[145]

This article explains it is futile to disagree.

Future Research: Prioritizing Consumer Trust

The broader one's understanding of the human experience, the better design we will have.—Steve Jobs[146]

From the plaintiff's perspective, traditional tort law benefits consumers by holding accountable parties responsible for injury, encouraging greater care in manufacture and ultimately making injured victims whole.

For defendants, traditional tort law offers the certainty required to proceed confidently through the product life cycle for all points of entry along the supply chain.

From insurers to investors, innovation entails risk levels that must be commensurate with opportunities to warrant the business endeavor.

Robotics and the AI-enabling robotic systems are the quintessential disruptive innovations spanning industries. No other technology has permeated so many industries with such transformative impact.

Whether traditional notions of legal responsibility comport with the advent of AI has been the sweetheart issue of academic research for decades. But less attention is given to the comparatively limited role traditional notions of learning patterns and brain functionality play in the dynamic landscape of robotic service products. How do robots decide? Does robotic choice resemble that of humans?

Studies in neuroimaging, organizational psychology, and systemic risk show decision making does not occur as often portrayed in popular cinema. Robots "learn" by amassing recognition for relevant data and "decide" by calculating the probability of a desired outcome based on the input received, as applied in numerous permutations of a given function.

Doctrinally, the human brain is not the ideal analogue to "machine learning." Yet more broadly, it is not entirely unfounded to appeal to consumers and foster trust in technology by espousing the idea that algorithmic decision making is not so foreign to human living.

Bypassing the broader question of whether robots can be liable in a literal sense, philosophical concepts of legal personhood are decidedly beyond the scope of this discussion. As originally conceived, the research supporting this article focused on the extent to which machine learning heightens robotic accountability and asked at what point ought the law hold robots liable because the decision creating the harm was not a function of software programming on the front end but a function of robotic choice—or algorithmic decision making?

In its first iteration, this article recommended a variation of Ugo Pagallo's "digital peculium" liability scheme for "hard cases" in which fully autonomous robots make decisions absent appropriate linkage to the original programmer outside the scope of pre-programmed uncertainty. Situating Pagallo's "hard cases" in the larger abstraction laid out by HLA Hart and Ronald Dworkin, this article concluded by considering whether determination of a right answer or conclusive indetermination of any exists for application of legal accountability to ever-increasing robotic autonomy. Among other reasons, advances in the global framework for automated driving necessitate an update.

Reflecting issues arising from the United Nations global framework for automated driving as well as developments in autonomous vehicle testing in the United States, future discussions shall be practical and the question more discrete: At what point ought the law hold supply chain actors liable as opposed to consumers because the decision creating the harm was not a function of consumer misuse but a failure of consumer education? Narrowing the question further, the next iteration operates wholly within the context of autonomous vehicles. But this future discussion also lends itself to extrapolation within the larger field of robotic liability.

The current iteration of this article prioritizes consumer education at the industry level and standardized nomenclature across jurisdictions. Analogizing to voluntary over-the-air software updates, which remain controversial in some circles, this article argues that voluntarily standardized nomenclature at the industry level is imperative for two reasons.

First, it is important for the certainty levels required to provide insurance for autonomous vehicles.

Second, it is a matter of good business. Selling the product and staying in business once the product is on the market presupposes consumer trust. Placing a premium on public education establishes the transparency needed to build consumer trust in innovative technologies.

Bibliography

Allen, Tom and Robin Widdison, "Can Computers Make Contracts?" (1996) 9 Harv JL & Tech 25.

Anderson, David L. and John C. Doyle, "Contrasting Views of Complexity and Their Implications for Network-Centric Infrastructures" (2010) 40 IEEE Transactions on Systems, Man and Cybernetics 839.

Asimov, Isaac, *I, Robot* (Gnome Press 1950).

Bonnelle, Valerie and others, "Individual Differences in Premotor Brain Systems Underlie Behavioral Apathy" (2015) Cerebral Cortex 1.

Burton, Lloyd and M. Jude Eagan, "Courting Disaster: Systemic Failures and Reactive Responses in Railway Safety Regulation" (2011) 20 Cornell JL & Pub Pol'y 533.

Damper, Robert I., "The logic of Searle's Chinese room argument" (2006) 16 Mind 164.

Dennett, Daniel, *The Intentional Stance* (MIT Press 1987).

D'Onfro, Jillian, "Google Is 'Re-thinking' All of Its Products to Include Machine Learning" *Business Insider* (October 22, 2015) http://www.businessinsider.com/google-on-machine-learning-2015-10, accessed November 26, 2020.

Dworkin, Ronald, *A Matter of Principle* (OUP 1985).

Dworkin, Ronald, *Law's Empire*, (Harvard University Press 1986).

Dworkin, Ronald, *Justice in Robes* (OUP 2006).

Fineman, Martha Albertson, "The Vulnerable Subject" (2008) 20 Yale J Law & Feminism 1.

Martha Albertson Fineman, "The Vulnerable Subject and the Responsive State" (2010) 60 Emory LJ 251.

Fineman, Martha Albertson and Anna Grear, *Vulnerability: Reflections on a New Ethical Foundation for Law and Politics* (Ashgate 2013).

Floreano, D. and others, *Automatic Creation of an Autonomous Agent: Genetic Evolution of a Neural-Network Driven Robot* (1994) Proceedings of the third international conference on simulation of adaptive behavior: From Animals to Animats 421.

French, Robert M., "Subcognition and the Limits of the Turing Test" in Stuart M. Shieber ed, *The Turing Test: Verbal Behavior as the Hallmark of Intelligence* (MIT Press 2004) 193-194.

Goldfeder, Mark, *Law and Technology*, Emory University School of Law (2015).

Hart, HLA, *The Concept of Law* (2d ed., Clarendon Press 1994).

Heyns, Christof, *2010 Report to the United Nations General Assembly*. Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions to the United Nations General Assembly.

Hoerzer, Gregor M. and others, "Emergence of Complex Computational Structures" (2014) Cerebral Cortex 678.

Howse, Robert, "Moving the WTO Forward—One Case at a Time" (2009) 42 Cornell Int'l LJ 223.

Jordan, M.I. and T.M. Mitchell, "Machine Learning: Trends, Perspectives and Prospects" (2015) 349 Science 255.

Karnow, Curtis E.A., "The Application of Traditional Tort Theory to Embodied Machine Intelligence" in Ryan Calo and others (eds) *Robot Law* (Edward Elgar Publishing 2016).

Legenstein, R. and others, "A reward-modulated Hebbian learning rule can explain experimentally observed network reorganization in a brain control task" (2010) 30 J Neuroscience 8400.

Marr, Bernard, "5 Ways Machine Learning Is Reshaping Our World" *Forbes* (October 22, 2015) https://www.forbes.com/sites/bernardmarr/2015/10/22/5-

ways-machine-learning-is-reshaping-our-world/?sh=49d7b316641a, accessed November 26, 2020.

Niccolai, James, "Google Says It's 'Rethinking Everything' around Machine Learning" *PC World* (October 23, 2015) https://www.pcworld.com/article/2996620/google-reports-strong-profit-says-its-rethinking-everything-around-machine-learning.html, accessed November 26, 2020.

Pagallo, Ugo, *The Laws of Robots: Crimes, Contracts, and Torts, Law Governance and Technology Series* 10 (Springer 2013).

Posner, Richard, *Economic Analysis of Law* (7th ed., Wolters Kluwer for Aspen Publishers 2007).

Potter, Norman, *What Is A Designer* (Hyphen Press 2002).

Giulio Prisco, "Susan Schneider on Machine Consciousness at the Upcoming Terasem Colloquium in Second Life" (*Turing Church*, December 4, 2015) http://turingchurch.com/2015/12/04/susan-schneider-on-machine-consciousness-at-the-upcoming-terasem-colloquium-in-second-life/, accessed November 27, 2020.

Raz, Joseph, *The Authority of Law: Essays on Law and Morality* (2d ed., OUP 2009).

Riedl, Mark, *Law and Technology Visiting Lecture*, Emory University School of Law (2015) https://eilab.gatech.edu/mark-riedl, accessed November 29, 2020.

Riedl, Mark, *The Lovelace 2.0 Test of Artificial Creativity and Intelligence*, Georgia Tech School of Interactive Computing and Director of Entertainment Intelligence Lab (2015) https://arxiv.org/abs/1410.6142, accessed November 29, 2020.

Ruhl, J.B., "Managing Systemic Risk in Legal Systems" (2013) 89 Ind LJ 559, 561.

Ruhl, J.B., "The Fitness of Law: Using Complexity Theory to Describe the Evolution of Law and Society and Its Practical Meaning for Democracy" (1996) 49 Vand L Rev 1407.

Russell, Stuart J. and Peter Norvig, *Artificial Intelligence: A Modern Approach* (Prentice Hall 1995).

Sartor, Giovanni, "Cognitive Automata and the Law: Electronic Contracting and the Intentionality of Software Agents" (2009) 17 Artificial Intelligence and Law 253.

Searle, John R, "Minds, Brains and Programs" (1980) 3 Behavioral and Brain Sciences 416.

Sheriff, Katherine D., Presentation: *Law and Technology*, Professor Goldfeder (2015).

Sheriff, Katherine D., *Professional Liability after Quantum Leaps in Technology: The Advent of Autonomous Vehicles and Technology's Uncertain Fit within Existing Tort Law* (2014).

Smith, Dave, "Technology's Next Big Frontier Is Teaching Machines to Learn from Their Own Mistakes" *Tech Insider* (October 23, 2015) http://

www.techinsider.io/what-is-machine-learning-2015-10, accessed November 26, 2020.

Solum, Lawrence, "Legal Personhood for Artificial Intelligence" (1992) 70 NC L Rev 1231.

Teubner, Günter, *Rights of non-humans? Electronic agents and animals as new actors in politics and law*, Max Weber Lecture at the European University Institute of Fiesole, Italy (January 17, 2007).

Thompson, Cadie, "The Real Problem with Artificial Intelligence" *Tech Insider* (September 17, 2015) https://www.businessinsider.com/autonomous-artificial-intelligence-is-the-real-threat-2015-9, accessed November 28, 2020.

Turing, Alan, "Computing Machinery and Intelligence" (1950) 59 Mind 433.

U.N. World Robotics (2005) *Statistics, market analysis, forecasts, case studies and profitability of robot investment*, ed U.N. Economic Commission for Europe and co-authored by the International Federation of Robotics, U.N. Publication Geneva Switzerland.

U.S. Supreme Court, *Lucas v. SC Coastal Council*, 505 U.S. 1003 (1992).

Vertinsky, Lisa, *The Role of Patents in International Public Health*, Emory University School of Law (2015).

Wolf, Gary, "Steve Jobs: The Next Insanely Great Thing, The Wired Interview" *Wired* (February 1, 1996) https://www.wired.com/1996/02/jobs-2/, accessed November 27, 2020.

Woolsey, R. James and Peter Vincent Pry, "The Growing Threat from an Electromagnetic Pulse (EMP) Attack" *Wall Street J* (August 12, 2014).

WP29 (2009) *The future of privacy*, EU Working Party art. 29 D-95/46/EC: WP 168 (December 1, 2009).

Notes

* Katherine D. Sheriff is a technology associate at Davis Wright Tremaine LLP devoting her legal practice to identifying areas of opportunity and potential challenges in emerging technology sectors, particularly in the dynamic fields of autonomous vehicles and artificial intelligence. She began writing this article in 2015 while at Emory Law School and has updated it since then to the point where it prioritizes consumer education at the industry level and standardized nomenclature across jurisdictions. Ms. Sheriff may be reached at katherinesheriff@dwt.com. (Endnotes are continued from Part I of this article.)

77. Pagallo, *The Laws of Robots* 104.

78. Giovanni Sartor, "Cognitive Automata and the Law: Electronic Contracting and the Intentionality of Software Agents" (2009) 17 Artificial Intelligence and Law 253.

79. Katherine D. Sheriff, Presentation: *Law and Technology*, Professor Goldfeder (2015).

80. Sheriff, Presentation: *Law and Technology*.

81. *Id.*

82. *Id.*

83. *Id.*

84. R. James Woolsey and Peter Vincent Pry, "The Growing Threat from an Electromagnetic Pulse (EMP) Attack" *Wall Street J* (August 12, 2014).

85. Sheriff, Presentation: *Law and Technology*.

86. Pagallo, *The Laws of Robots* 184; Norman Potter, *What Is A Designer* (Hyphen Press 2002).

87. Pagallo, *The Laws of Robots* 185-186.

88. *Id.* at 186-187.

89. *Id.* at 188.

90. *Id.*

91. *Id.*

92. *Id.*

93. *Id.*

94. *Id.* (emphasis added).

95. *Id.* at 188-189.

96. *Id.*

97. *Id.* at 15.

98. *Id.*

99. *Id.*; Richard Posner, *Economic Analysis of Law* (7th ed., Wolters Kluwer for Aspen Publishers 2007) 180.

100. Pagallo, *The Laws of Robots* 15.

101. J.B. Ruhl, "Managing Systemic Risk in Legal Systems" (2013) 89 Ind LJ 559, 561.

102. Ruhl, "Managing Systemic Risk" 564.

103. *Id.*; David L. Anderson and John C. Doyle, "Contrasting Views of Complexity and Their Implications for Network-Centric Infrastructures" (2010) 40 IEEE Transactions on Systems, Man and Cybernetics 839.

104. Ruhl, "Managing Systemic Risk" 562; Anderson and Doyle, "Contrasting Views of Complexity" 839.

105. *Id.*

106. Martha Albertson Fineman, "The Vulnerable Subject" (2008) 20 Yale J Law & Feminism 1; Martha Albertson Fineman, (2010) "The Vulnerable Subject and the Responsive State" 60 Emory LJ 251.

107. Martha Albertson Fineman and Anna Grear, *Vulnerability: Reflections on a New Ethical Foundation for Law and Politics* (Ashgate 2013) 33-34.

108. Fineman and Grear, *Vulnerability* 34-35.

109. *Id.* at 35.

110. *Id.* at 39-40.

111. *Id.*

112. *Id.* at 42-43.

113. Ruhl, "Managing Systemic Risk" 574; Robert Howse, "Moving the WTO Forward—One Case at a Time" (2009) 42 Cornell Int'l LJ 223; J.B. Ruhl, "The Fitness of Law: Using Complexity Theory to Describe the Evolution of Law and Society and Its Practical Meaning for Democracy" (1996) 49 Vand L Rev 1407.

114. Ruhl, "Managing Systemic Risk" 574; Robert Howse, "Moving the WTO Forward—One Case at a Time" 223.

115. Ruhl, "Managing Systemic Risk" 574; *Lucas v. SC Coastal Council*, (1992) 505 US 1003, 1031.

116. Ruhl, "Managing Systemic Risk" 601-602; Lloyd Burton and M. Jude Eagan, "Courting Disaster: Systemic Failures and Reactive Responses in Railway Safety Regulation" (2011) 20 Cornell JL & Pub Pol'y 533.

117. Ruhl, "Managing Systemic Risk" 601; Burton and Egan, "Courting Disaster" 558-561.

118. WP29 (2009) *The future of privacy*, EU Working Party art. 29 D-95/46/EC: WP 168 (December 1, 2009); UN World Robotics (2005) *Statistics, market analysis, forecasts, case studies and profitability of robot investment*, ed UN Economic Commission for Europe and International Federation of Robotics, UN Publication Geneva Switzerland.

119. Pagallo, *The Laws of Robots* 179-180.

120. *Id.* at 179.

121. *Id.*

122. *Id.* at 179-180.

123. *Id.* at 180.

124. HLA Hart, *The Concept of Law* (2d ed., Clarendon Press 1994) 128.

125. Pagallo, *The Laws of Robots* 180.

126. *Id.*

127. *Id.*

128. Pagallo, *The Laws of Robots* 180; Ronald Dworkin, *A Matter of Principle* (OUP 1985).

129. Pagallo, *The Laws of Robots* 180; Ronald Dworkin, *A Matter of Principle* 159.

130. Pagallo, *The Laws of Robots* 180; Ronald Dworkin, *Justice in Robes* (OUP 2006), 266; Joseph Raz, *The Authority of Law: Essays on Law and Morality* (2d ed., OUP 2009).

131. Pagallo, *The Laws of Robots* 180.

132. *Id.*

133. Pagallo, *The Laws of Robots* 180; Ronald Dworkin, *Law's Empire*, (Harvard University Press 1986), 412.

134. Pagallo, *The Laws of Robots* 181.

135. Pagallo, *The Laws of Robots* 45; Christof Heyns, *2010 Report to the United Nations General Assembly*.

136. Pagallo, *The Laws of Robots* 181-182; Heyns, *2010 Report to the United Nations General Assembly*.

137. Pagallo, *The Laws of Robots* 188; Karnow, "Liability for distributed artificial intelligence" 147.

138. Pagallo, *The Laws of Robots* 15; Posner, *Economic Analysis of Law* 180.

139. Pagallo, *The Laws of Robots* 188; Teubner, *Rights of non-humans? Electronic agents and animals as new actors in politics and law*.

140. Pagallo, *The Laws of Robots* 189-191.

141. *Id.* at 191-192.

142. *Id.* at 16-17.

143. Isaac Asimov, *I, Robot* (Gnome Press 1950).

144. Pagallo, *The Laws of Robots* 16-17.

145. *Id.* at 17.

146. Gary Wolf, "Steve Jobs: The Next Insanely Great Thing, The Wired Interview" *Wired* (February 1, 1996) https://www.wired.com/1996/02/jobs-2/, accessed November 27, 2020.