SYMPOSIUM

RISE OF THE MACHINES: ARTIFICIAL INTELLIGENCE, ROBOTICS, AND THE REPROGRAMMING OF LAW

FOREWORD

Deborah W. Denno & Ryan Surujnath***

INTRODUCTION

This Foreword provides an overview of *Rise of the Machines: Artificial Intelligence, Robotics, and the Reprogramming of La*w, a symposium hosted by the *Fordham Law Review* and cosponsored by the Fordham Law School's Neuroscience and Law Center. As the Symposium spotlights, artificial

* Arthur A. McGivney Professor of Law, Founding Director, Neuroscience and Law Center, Fordham University School of Law.

** Analyst, GSO Capital Partners, The Blackstone Group Inc.; J.D., 2018, Fordham University School of Law. This Foreword discusses the *Fordham Law Review* Symposium entitled *Rise of the Machines: Artificial Intelligence, Robotics, and the Reprogramming of Law* (cosponsored with Fordham Law School's Neuroscience and Law Center), held at Fordham Law School. We are most grateful to the Symposium participants for their insightful presentations and their superb articles published in this issue. We also thank the members of the *Fordham Law Review* for their incredible care and thought in organizing the Symposium and the editorial process, especially Andrew Kirschenbaum, Lauren Gorab, Sean O'Grady, Lauren Knoke, and Jane Ramage. There are many invaluable behind-the-scenes individuals who made this Symposium possible. They include Rick Turk, who offered wonderful advice and encouragement, as well as Shanelle Holley, Morgan Benedit, Victoria Grantham, and Robert Yasharian, all of whom expertly publicized the Symposium and managed many of the details associated with it. Jacob Fishman and Erica Valencia-Graham provided outstanding comments and research assistance for this Foreword. Finally, we truly appreciate Dean Matthew Diller's steadfast support and inspiration as well as the indispensable contributions of the Neuroscience and Law Center's Board of Advisors. We are indebted to six sources for research funding: Fordham University School of Law, Fordham's Neuroscience and Law Center, Mr. and Mrs. John R. Costantino, the Gerald M. Edelman Post-Graduate Fellowship in Neuroscience, Roger Sachs Family Foundation, and the Barnet and Sharon Phillips Family Fund.

intelligence[1] (AI) and robotics[2] are no longer the products of science fiction. AI is used by millions of people every day, from hedge fund managers to health-care professionals and even consumers of personalized assistants like Siri, Cortana, and Alexa.[3] Neuroscience—"the branch of life sciences that studies the brain and nervous systems,"[4]—is integral to AI development, as programmers seek to improve machines by understanding human thought patterns.[5]

1. There is no uniform or generally approved definition of artificial intelligence. *See* Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. DAVIS L. REV. 399, 404 (2017). Mainly, the term is regarded "as a set of techniques aimed at approximating some aspect of human or animal cognition using machines." *Id*.; *see also* Tabrez Y. Ebrahim, *Data-Centric Technologies: Patent and Copyright Doctrinal Disruptions*, 43 NOVA L. REV. 287, 295 (2019) (defining artificial intelligence as "a program running on a computer system that is able to learn and adapt itself in a dynamic environment"); Milan Markovic, *Rise of the Robot Lawyers?*, 61 ARIZ. L. REV. 325, 329 (2019) ("Although definitions of artificial intelligence vary, the term is generally associated with the automation of intelligent behavior via computer processes."). Stuart Russell and Peter Norvig stress the importance of an "intelligent" agent, thereby viewing artificial intelligence "as the study of agents that receive percepts from the environment and perform actions." STUART RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH, at viii (3d ed. 2010).

2. There is no consensus concerning how "robot" or "robotic" should be defined. *See* F. Patrick Hubbard, *"Sophisticated Robots": Balancing Liability, Regulation, and Innovation*, 66 FLA. L. REV. 1803, 1807 (2014). Indeed, the terms "robotic" and "artificial intelligence" are frequently treated synonymously. *See* Mark A. Lemley & Bryan Casey, *Remedies for Robots*, 86 U. CHI. L. REV. 1311, 1321 (2019). That said, there is an overall view that "robots are mechanical objects that take the world in, process what they sense, and in turn act upon the world." Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. 513, 529–30 (2015). This "sense-think-act paradigm" differentiates robots from other technical devices. For example, while a laptop with a camera can "sense and process the external world" to a certain extent, the laptop camera "does not act upon the world." *Id*.; *see also Robotics*, TECHOPEDIA, https://www.techopedia.com/definition/32836/robotics [https://perma.cc/9VAQ-C2BU] (last visited Oct. 6, 2019) (Robotics refers to "the engineering, construction and operation of robots" to perform tasks or play a role in various commercial and consumer uses.); *Robots and Robotic Devises—Vocabulary*, INT'L ORG. FOR STANDARDIZATION, https://www.iso.org/obp/ui/#iso:std:iso:8373:ed-2:v1:en [https://perma.cc/BQ8C-WG5R] (last visited Oct. 6, 2019) (defining "robotics" as the "science and practice of designing, manufacturing, and applying robots").

3. *See* Fei Jiang et al., *Artificial Intelligence in Healthcare: Past, Present and Future*, 2 STROKE & VASCULAR NEUROLOGY 230 (2017) (noting that AI is used by health-care professionals); Erik Brynjolfsson & Andrew McAfee, *The Business of Artificial Intelligence: What It Can–and Cannot–Do for Your Organization*, HARV. BUS. REV. (July 18, 2017), https://hbr.org/cover-story/2017/07/the-business-of-artificial-intelligence [https://perma.cc/Y2WY-YQPL] (noting that AI is used by millions of people every day); *Hedge Funds Embrace Machine Learning—Up to a Point*, ECONOMIST (Dec. 9, 2017), https://www.economist.com/finance-and-economics/2017/12/09/hedge-funds-embrace-machine-learning-up-to-a-point [https://perma.cc/7GUY-7GXE] (noting that AI is used by hedge fund managers); Rufin VanRullen, *Perception Science in the Age of Deep Neural Networks*, FRONTIERS PSYCHOL. (Feb. 2, 2017), https://www.frontiersin.org/articles/10.3389/fpsyg.2017.00142/full [https://perma.cc/26KK-YN6W] (explaining that AI is used by consumers of personalized assistants like Siri, Cortana, and Alexa).

4. NEUROSCIENCE AND THE LAW: BRAIN, MIND, AND THE SCALES OF JUSTICE 206 (Brent Garland ed., 2004); *see also* OWEN D. JONES ET AL., LAW AND NEUROSCIENCE 762 (2014) (defining neuroscience as "[t]he scientific study of the structure and function of the nervous system; includes experimental and clinical studies of animals and humans").

5. *See generally* Jacob T. Schwartz, *The New Connectionism: Developing Relationships Between Neuroscience and Artificial Intelligence*, DAEDALUS, Winter 1988, at 123 (predicting,

During the early stages of AI, neuroscience was integral to the development of basic neural networks' reinforcement learning. Today, modern AI research has taken cues from neurological studies to replicate human cognitive functions in an AI's code. For example, one challenge facing modern AI is continual learning, which is the ability to master a new task without forgetting old ones. Cutting-edge neuroimaging techniques allow scientists to study plasticity in the brain's neocortex during human continued learning; in AI research, this development has led to the creation of new deep-learning neural networks that solve the catastrophic forgetting problem. As a practical matter, the use of neuroscience in AI development seems to be leading to machines that can learn quickly and without thought instead of having to be "retaught" through costly and processing-intensive cloud computers.

The pace of today's research is rapid and fueled by advancements beyond pure software: "neurorobotics" is a field born from the combination of neuroscience, robotics, and AI.[6] Neurorobotics devices use biologically inspired neural networking systems which are implemented into physical platforms. In turn, such devices are integral to the development of industrial-grade robotics, prosthetics, and even primitive nanomachines. Just as these technologies promise to reinvent industry, our traditional understanding of legal rules and systems could be at the precipice of major change.

Nonetheless, AI is something of a buzzword across the legal industry. There is still a certain mystique to the technology's functionality that this Symposium intended to clarify while also assessing how it can affect legal regimes. In particular, this Symposium focused on problems posed by current and very near-future AI research and development with the aim to facilitate a dialogue among those who will shape the future of this impactful technology: neuroscientists, computer scientists, attorneys, and business professionals. As researchers continue to use neuroscience to make AI more "human" in its reasoning, the technology has encountered a range of human legal problems, including discrimination and bias, civil liability for risk-taking, and ownership of data and creative content.

Variants of the technology are also being used across many disciplines. Arguably, nowhere is the technology's application more prominent than in the financial services sector. AI is part of a new wave of cost-reducing financial technologies—all of which have the potential to change the way people and institutions interact with capital. At the same time, these

---

in 1988, a surge of growing interest by the computer science community in experimental neuroscience and the insights it will produce).

6. *See* Marco Iosa et al., *The Three Laws of Neurorobotics: A Review of What Neurorehabilitation Robots Should Do for Patients and Clinicians*, 36 J. MED. BIOLOGICAL ENGINEERING 1, 2 (2016) ("Neurorobotics refers to the branch of science combining neuroscience, robotics, and artificial intelligence. It hence refers to all robots developed for interacting with or for emulating the nervous systems of humans or other animals."); *see also* Frederic Kaplan, *Neurorobotics: An Experimental Science of Embodiment*, FRONTIERS NEUROSCIENCE (Aug. 1, 2008), https://www.frontiersin.org/articles/10.3389/neuro.01.023.2008/full [https://perma.cc/S7T3-RNJ7] ("At the interface of neuroscience and robotics, neurorobotics is the science and technology of embodied autonomous neural systems.").

machines threaten to multiply existing financial risks or to create entirely new ones.

Regardless of the industry, ethical standards for the development of AI will be crucial. There is a popular adage in the world of computing: "garbage in, garbage out." In essence, this idea tells us that flawed inputs will yield flawed results. It is an unfortunate reality that human beings are imperfect and susceptible to errors, biases, and prejudices. It is thus integral to reduce the impact that human judgments have on the tools we use. The transition to a world of algorithmic governance is not without its potential costs. As is particularly salient in the national discourse, it appears that our privacy is something of a premium. With the next great advancement in automated decision-making, individuals may stand to lose in privacy what they gain in convenience.

I. HOW NEUROSCIENCE AND ETHICS INFORM ROBOTS AND THE LAWS GOVERNING THEM

AI and robotics are at the forefront of tomorrow's algorithmic society. Thanks to the latest neuroimaging devices, modern neuroscience has revealed deep insights into human reasoning and cognition. Some of the most promising developments in AI research are inspired by neuroscience. Deep learning and reinforcement learning, two foundational pieces of modern AI development, attempt to replicate neurological communication mathematically. As AI is used for more complex tasks, it stands to benefit from even more nuanced understandings of human reasoning.

This Symposium starts with some of the big-picture trends in modern AI and robotics research, especially those pertaining to the influence of neuroscience. Stunningly, robots and AI algorithms have demonstrated cognitive reasoning capabilities to the extent that they can replicate creative pursuits, like art and music. The notion of legal personhood for AI systems has become a less far-fetched proposition in light of advances in the technology that mirror (if only rudimentarily so) certain aspects of the human thought process. This begs the question of what kinds of legal regimes and techniques will be best suited for dealing with questions of liability.

Iria Giuffrida confronts these issues directly by examining the legal consequences of the construction and marketing of AI systems—especially when "technical advancements have outpaced legal actions"[7]—while also considering whether the problems with AI merit a revised perspective with respect to liability.[8] For example, the surge in AI has been cultivated in part by developments in machine learning, which pertain to an AI system's capacity to alter itself by allowing for new data[9] with which it can pinpoint patterns for purposes of prediction.[10] While AI can examine vast amounts of

7. Iria Giuffrida, *Liability for AI Decision-Making: Some Legal and Ethical Considerations*, 88 FORDHAM L. REV. 439, 440 (2019).

8. *Id*.

9. *Id*. at 441.

10. *Id*.

data, "[t]he risk of AI error is huge,"[11] especially if the AI system takes in data that is biased and fallacious.[12] Indeed, even a correctly designed starting program "may modify its 'understanding' to accept the biased or false information as accurate and perform its function based on that erroneous data."[13]

This fallible "AI Ecosystem" has created a complex combination of legal rules; yet, Giuffrida's major interest concerns liability risks especially considering the vast array of potentially responsible parties who could get involved when a problem occurs.[14] As she explains, "[t]here are AI developers; algorithm trainers; data collectors, controllers, and processors; manufacturers of the devices incorporating the AI software; owners of the software (which are not necessarily the developers)"; and of course the consumers and users of the products who also could be highly varied and layered.[15]

Giuffrida's primary concern is whether these kinds of questions warrant a revised solution to liability, and her potential solutions are fourfold.[16] The first solution is to provide AI with legal personhood,[17] which would mandate that the AI system be able to hold assets either directly (like a corporation) or indirectly (like a licensor or licensee of the AI system acting on the system's behalf).[18] In this capacity, the AI system's liability risk would differ based on "the nature of the AI," such as whether or not it is located in a physical object,[19] as well as the AI system's purpose. For example, there are predictive systems that aid human decision-making, as well as fully autonomous systems that do not involve human input.[20] In this context, any harm that the AI system causes could be a direct result of how the AI is programmed, thus potentially creating an intentional tort based on "negligent design, training, or operation (e.g., lack of adequate cyber security protections); or an arguably unforeseeable harm caused by an interaction with unforeseeable real-world data."[21] Indeed, Giuffrida provides several examples of how risk, causation, and responsibility could pose challenges in assessing AI cases.[22]

Giuffrida's second solution is to "leave AI alone,"[23] which assumes that the major question should be "by what standard should we determine liability when unacceptable harm occurs but its causation cannot be determined," especially in situations where there is minimal human oversight of the

11. *Id*. at 442.
12. *Id.*
13. *Id*.
14. *Id*. at 443.
15. *Id*.
16. *Id*. at 444.
17. *See id*.
18. *Id*.
19. *Id*. at 444–45.
20. *Id*. at 445.
21. *Id*.
22. *See id*. at 446–47.
23. *Id.* at 447.

system's decisions or predictions.[24] The recommendations proposed for self-driving cars are good examples, and Giuffrida highlights an especially appealing one—the use of a mandatory no-fault type of insurance process in which a victim injured by a self-driving car is paid a certain sum without the need to establish how the car caused the victim's injury.[25]

The third solution may be to view "the harm as a necessary societal cost" and adopt "robot common sense."[26] Giuffrida provides as an example a Wisconsin Supreme Court decision, *State v. Loomis*,[27] which upheld a judge's use of COMPAS, an AI predictive device, in determining the defendant's sentence.[28] The court stressed that it was the judge—not the AI—that sentenced the defendant and that the COMPAS device was only one of a number of factors that the judge considered.[29] Yet the concept of robot common sense raises an underlying principle. While judicial sentencing is inherently flawed, technologically enhanced sentencing "has at least the possibility of improving over time and curing the current—and defective—human system."[30]

The fourth solution is a harms-based approach, which would make the "compensation-deterrence methodology" harm-specific rather than tortfeasor-specific. Thus, the harm created by self-driving cars may be more feasibly covered by a no-fault compensation system if the cars have inherent risks associated with them.[31] That said, while this solution may be appealing to those companies that would prefer to internalize the costs of liability rather than change their products,[32] critics contend that companies will instead take the risk and spread the predicted cost of liability to consumers. In turn, there would be little financial motivation for companies to avoid harm.[33] Regulation may be an alternative to tort suits, but it also has complications.[34] Regardless of the approach, Giuffrida stresses that "we must unavoidably deal with a cost-benefit analysis."[35]

Giuffrida offers a new approach to these four solutions. Instead of proposing a compensatory system for AI harms, she recommends focusing on "identifying and dissuading (and perhaps compensating) the major predictive harms, with the understanding that constant reevaluation will be necessary."[36] In addition, recent ethical codes directed toward AI systems could provide some guidance. These include the 2018 adoption by the European Commission for the Efficiency of Justice of the Council of Europe

24. *Id*. at 448.
25. *Id*. at 448–49.
26. *Id*. at 449.
27. 881 N.W.2d 749 (Wis. 2016).
28. Giuffrida, *supra* note 7, at 449–50.
29. *Id*. at 449.
30. *Id.* at 450.
31. *Id*.
32. *Id*. at 452.
33. *Id*.
34. *Id*.
35. *Id*.
36. *Id*. at 453.

of the European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems.[37] In addition, the High-Level Expert Group on AI appointed by the European Commission published the final version of its Ethics Guidelines for Trustworthy AI in mid-2019.[38] Likewise, the Beijing Academy of Artificial Intelligence released the Beijing AI Principles, which were followed in July 2019 by the Governance Principles for the New Generation Artificial Intelligence and published by the National Governance Committee for the New Generation Artificial Intelligence. As Giuffrida notes, the Beijing AI Principles seem to recommend that AI developers seek informed consent before buyers use their products, thereby suggesting the potential for data protection measures similar to those provided by European countries.[39]

The United States has gone in a different direction. While Executive Order 13,859 of February 2019 "clearly encourages the development of American AI," it fails to refer to ethics.[40] The Algorithmic Accountability Act of 2019 demonstrates congressional concern with regulating AI and it includes an emphasis on bias in AI decision-making; yet it does not make itself obliged to particular ethical values.[41] In contrast, private entities, such as Big Tech, are developing a framework for an ethical AI system, exemplified by Google's decision to avoid a contract in which the military could use their AI advances.[42] In a nutshell, the U.S. solution is mostly privately driven.[43]

Giuffrida concludes that, while some type of AI system regulation "is inevitable," the most important concerns are those related to the ethics of AI systems. In addition to greater transparency and explanation, "the best models" will derive "from interdisciplinary efforts."[44]

Along with Giuffrida, Gerhard Wagner points out that, currently, robots and other autonomous systems do not have personhood and their owners are typically responsible for them.[45] The European Parliament predicts that, at some point, there will be a "special legal status for robots"—seemingly as "electronic persons" or "ePersons"[46] that would be responsible for any damage they caused, most likely under tort law. Yet, Wagner questions whether such a reclassification "makes sense."[47] For example, personhood requires a range of criteria, such as consciousness, self-awareness, and mental and emotional capacity; yet there is no firm consensus regarding which of these criteria are necessary conditions for acknowledging

37. *Id*. at 454.
38. *Id*.
39. *Id*. at 455.
40. *Id*. at 456.
41. *Id*.
42. *Id*.
43. *Id*.
44. *Id*.
45. Gerhard Wagner, *Robot, Inc.: Personhood for Autonomous Systems?*, 88 FORDHAM L. REV. 591, 592 (2019).
46. *Id*.
47. *Id*. at 593.

consciousness.[48] Not only are the features of personhood "a matter of degree,"[49] rather than "either/or," but the primary feature "is the ability to act as an autonomous subject."[50] In addition, philosophical approaches to personhood diverge from legal ones. Wagner notes, for example, that consequentialist approaches, such as utilitarianism, emphasize "whether autonomous systems qualify as sentient beings capable of feeling pleasure and pain"[51] (a reigning utilitarian argument in the realm of animal rights).[52] In turn, "the criteria used by the legal system to define personhood are primarily biological."[53]

Wagner also questions whether robots and other autonomous devices can be regarded as "liability subjects,"[54] a matter based primarily on "whether there are good reasons to treat them like as legal persons."[55] Those "good reasons" derive from a similar framework delineating the personhood status of corporations: they will be predominantly economic[56] and focused on whether robots "qualify as wrongdoers" and not on how much they resemble human beings.[57] Wagner's determination depends on an economic calculus: "[t]he objective is to maximize the net surplus for society, i.e., the difference between the gain from activities involving robots and the costs of producing and operating them, including the costs of precautions and the costs of accidents that occur in spite of cost-effective precautions."[58]

In support of his approach, Wagner specifies liability frameworks for two "distinct groups" of liability subjects, namely manufacturers and users, to gauge where robot liability could fall[59] as well as the method of risk allocation through contract.[60] According to Wagner, robot technology will move the control over the machines and appliances away from the users to the manufacturers,[61] in which case manufacturers of robots will have substantially more power over robots than the manufacturers of mechanical products currently possess.[62] Such control will be particularly evident where a closed software system is in place because only the manufacturer will be able to expand the device's safety features, for example.[63] In contrast, in an open-system approach, the assignment of responsibilities may be far more complex given the numbers and types of parties involved, including the first set of equipment manufacturers and the many suppliers of component parts,

48. *Id*. at 594.
49. *Id*. at 595.
50. *Id*.
51. *Id*. at 596.
52. *Id*. at 596–97.
53. *Id*. at 598.
54. *Id*. at 599.
55. *Id*.
56. *Id*. at 600.
57. *Id*.
58. *Id*.
59. *Id*. at 601.
60. *Id*.
61. *Id*. at 602.
62. *Id*.
63. *Id*. at 602–63.

such as owners and operators.[64] Therefore, classifying the robot as an "ePerson" would "relieve the victim of the burden of identifying the responsible party and would spare courts the task of allocating liability between a multitude of defendants."[65]

In essence, robots and other autonomous systems will introduce new complications for standard tests of products liability, including the consumer expectations and risk utility products liability tests,[66] as well as to the legal system's current understanding of design defect.[67] Wagner therefore suggests "a system-oriented concept of design defect" in which the major focus will be whether the system at issue "causes an unreasonable number of accidents overall."[68] Nonetheless, Wagner also recognizes that such an approach will create problems for competition in the marketplace because it may force a situation in which the finding of a design defect may be based on an "'optimal algorithm test' that discriminates against all but the best algorithm in the market."[69] In addition, the users of robots and other autonomous systems should operate with a restricted duty of care because they will possess only very limited control over the devices they manage.[70]

Wagner takes time to assess the advantages and disadvantages of accepting robots as legal entities that have liability.[71] A powerful disadvantage is that robots are unable to pay damage claims.[72] Likewise, if robots were ePersons, all the actors involved in the robot's creation would be protected from liability[73] and injured victims would not be compensated.[74] One suggestion to counter this scenario is to require either that robots possess "a minimum of assets in order to qualify as a legal entity" or that they be accompanied with mandatory liability insurance.[75] The drawback is that these costs, if incurred by manufacturers, would be passed on to the users.[76]

Wagner is skeptical about how much robots will be able to accommodate a liability system irrespective of these proposed solutions. Even if robots were programmed to "learn" from past accidents and experiences and algorithmically adjust themselves accordingly, the capacity for this software improvement would still be controlled by the decisions made by software programmers.[77] Yet, because "potential ePersons are unreceptive to financial incentives to avoid harm" in the way humans are, Wagner perceives

64. *Id*. at 603.
65. *Id*.
66. *Id*. at 605.
67. *Id*.
68. *Id*. at 606.
69. *Id*.
70. *Id*. at 607.
71. *Id*. at 593.
72. *Id*. at 609.
73. *Id*.
74. *Id*.
75. *Id*. at 610.
76. *See id*.
77. *Id*. at 611.

problems with respect to deterring robots' injurious behavior "even if minimum asset requirements or insurance mandates apply."[78]

In essence, then, Wagner concludes that there is little to be gained by making robots ePersons.[79] From an economic perspective, making the ePerson liable would result in only limited liability of its manufacturers and users.[80] That said, if robots and autonomous systems succeed in producing the "great savings in accident costs that they are promised to, then no liability subsidy is needed" and there may be advantages to designating them ePersons after all.[81]

II. AI, ETHICS, AND FINANCIAL MARKETS: THE RISKS FACED ON WALL STREET AND MAIN STREET

The Symposium's second group of articles focuses on the impact of AI on the financial services sector. Big money players like asset managers and banks have been aggressive investors in the technology, aiming to capture value realized by other industries, while remaining wary of reputational and regulatory pitfalls. Finance has a lengthy history with predictive technology, which dates back to the industry's dalliances with algorithmic and high-frequency trading.

Today, financial firms also envision AI as a means to lower costs and improve customer relations across entire organizations. The upsides are tantalizing for institutions and customers alike. Robo-advisors, for example, offer automated investment advice that can provide inexperienced retail investors with no need for an investment manager with low-cost access to capital markets. Managers, on the other hand, can devote their human resources to more complex accounts or strategies that demand human reasoning (and higher fees). The integration of AI into finance can theoretically offer high margins and new profit opportunities for Wall Street. For consumers on Main Street, financial technology has promised lower-cost services and greater access to lending for groups typically underserved by traditional finance.

There are risks, however, and the real-world integration of AI in this space can often fall far short of the ideal. Overreliance on automated decision-making exacerbates systemic financial risks. Meanwhile, consumers taking advantage of new-age, AI-enabled services risk exposure to potentially predatory or discriminatory lenders. The role of AI in finance has been both profitable and socially desirable yet also detrimental in many ways.[82]

According to Tom C.W. Lin, there are "four inherent areas of intertwined risks and limitations relating to programming codes, data bias, virtual threats,

78. *Id*.
79. *Id*. at 611–12.
80. *Id*.
81. *Id*. at 612.
82. Tom C.W. Lin, *Artificial Intelligence, Finance, and the Law*, 88 FORDHAM L. REV. 531, 532 (2019).

and systemic risks."[83] The first risk concerns the limitations of AI code and the inherent unpredictability of markets. Lin argues that AI programs are thus far unable to accurately model the key risks in the marketplace.[84] Lin suggests that market risks warrant consideration beyond pure mathematics; communication in boardrooms or on trading floors is ultimately conducted by humans, complete with flawed and nuanced cues that are unable to be captured in code.[85] Lin notes the industry's tendency to ignore this proposition and place blind faith into these "infallible" machines, citing the 2008 financial crisis as a consequence of this thinking.[86]

The second risk, which deals with discriminatory data and algorithmic biases, raises the need to recognize the kinds of latent prejudices that exist in data so that they do not contribute to algorithmic distortions against certain individuals or groups.[87] As Lin stresses, it is imperative that AI systems do not introduce past or present discrimination into future technology "under the blended gloss of innovation, neutrality, and objectivity."[88]

The third risk pertains to cybersecurity risks posed by both external and internal parties.[89] External system breaches can range from simple acts of theft to state or nonstate actors attempting to disrupt the American financial infrastructure. Meanwhile, preexisting internal threats posed by actors like disgruntled employees or corporate spies can take on greater magnitude due to the speed at which monetary transfers now occur.[90] Because such threats have become more imperceptible, they are more challenging to prevent and defeat,[91] and these problems will grow only more daunting as the financial industry increases its reliance on AI.[92]

The fourth risk deals with the systemic perils and financial mishaps associated with the growing use of financial AI and technology.[93] These risks relate to the growing size of financial institutions (which carries with it more risks), their increasing speed (which enables greater disruptions in the system before corrections can be introduced), and linkages among firms (which allow errors in one system to destabilize other systems as well).[94] The result, Lin warns, can be a system of institutions that possess too much data to fail and that operate too quickly for humans to mitigate financial accidents.[95]

---

83. *Id*. at 533.
84. *Id*. at 534.
85. *Id*. at 535.
86. *Id.*
87. *Id*. at 536–37.
88. *Id*. at 538.
89. *See id*.
90. *See id*. at 539.
91. *Id*. at 540.
92. *Id*.
93. *Id*. at 541.
94. *See id*. at 542.
95. *Id*. at 541.

In light of these risks, Lin investigates possible responses,[96] especially with respect to financial cybersecurity[97] and the private parties who may have competing interests regarding their control of the "global cyberinfrastructure."[98] As Lin stresses, public policymakers must start to provide global incentives for private firms to "cooperate better with other firms and public regulators" in light of the increasingly ominous threats of cybersecurity attacks.[99] Likewise, because financial AI will heavily influence competition within the financial industry, firms with larger data sets may have competitive advantages in the marketplace that can impair consumer welfare and the health of the financial landscape.[100] As a result, policymakers must be aware of such hazards and their implications.[101]

Lastly, the growth of financial AI will influence individuals and society alike regarding the role humans will have in finance as well as what role finance will have in society, including shared values such as equal access and transparency.[102] Such goals will be challenging given the clash between old and new politics and the diverse approaches to regulating new financial technology.[103] Ensuring the role of human participants is imperative[104] to maintaining "the people-centered, social purposes of finance."[105] Thus, the evolution of financial AI—with all of its power and potential—can also harm individuals.[106] The key goal "is to create better financial artificial intelligence—one that is less artificial, more intelligent, and ultimately more humane, and more human."[107]

Although Lin notes the systemic risks associated with the use of AI in traditional finance, individuals can face more direct risks. Kristin Johnson, Frank Pasquale, and Jennifer Chapman's essay concerns the growth and potential dominance of financial technology ("fintech") firms.[108] Fintech firms incorporate the advantages garnered by learning algorithms—a type of AI—to decrease transaction fees and increase interest rates on deposits and other payments.[109] Compared to the established legacy firms, which initially eschewed mobile banking, fintech firms can better find and service consumers by more accurately evaluating consumer creditworthiness and assessing business risks.[110] In addition, by using facially neutral, objective

96. *Id*. at 533.
97. *Id*. at 543.
98. *Id*. at 544.
99. *Id*. at 545.
100. *Id*.
101. *Id*. at 548.
102. *Id*. at 548–50.
103. *Id*.
104. *Id*.
105. *Id*.
106. *Id*. at 551.
107. *Id*.
108. Kristin Johnson, Frank Pasquale & Jennifer Chapman, *Artificial Intelligence, Machine Learning, and Bias in Finance: Toward Responsible Innovation*, 88 FORDHAM L. REV. 499, 499–500 (2019).
109. *Id*. at 501.
110. *Id*.

criteria, the learning algorithms mitigate creditors' exposure to claims of intentional or unintentional discrimination against borrowers who are members of legally protected classes.[111] According to the authors, however, in 2018 the Office of the Comptroller of the Currency (OCC) undermined this goal by allowing fintech firms to apply for special national banking charters, which allow them to evade important state consumer finance regulations, including those on payday lending and usury.[112]

This essay questions the presumption that, through the use of learning algorithms, fintech firms help marginalized and low-income individuals by emphasizing two grave concerns. First, the authors contend that AI-driven platforms that fintech firms rely on may mirror the biases of their programmers or input data, thereby fueling discrimination against members of legally protected classes.[113] Second, the devices that machine learning algorithms use to identify and service marginalized and low-income consumers may also be used to single them out. There are legal and ethical implications to either of these outcomes: not only may the fintech firms be contravening equal access credit statutes, they could also further marginalize legally protected groups and low-income individuals who are often victims of predatory tactics.[114]

The authors contend that, although fintech firms initially celebrated the advances in access to financial services brought by learning algorithms, there have been dangerous unintended consequences.[115] For example, even though the facially neutral learning algorithms eliminate biases that can come from face-to-face decisions in financial services, there is evidence that incomplete or inaccurate data sets may distort the algorithms' objectivity. In addition, the quest by such algorithms to seek the most efficient path to solve a problem may result in targeting a purportedly neutral attribute in data sets that may in fact be a proxy for a legally protected trait. Therefore, such an approach may produce a discriminatory outcome regardless of whether the program developers intended to create an algorithm that should not discriminate based on that very same trait.[116] As the authors underscore, overlooking the potential for such biases "may weaponize [automated decision-making platforms]"[117] and further hinder the effectiveness of accountability standards. These dangers are especially evident in light of recently adopted federal banking regulations that may support such advances "but leave the most marginalized individuals and families deeply vulnerable to exploitation and discrimination as fintech firms dominate the financial markets."[118]

---

111. *Id*. at 505.
112. *Id*.
113. *Id*.
114. *Id*. at 510.
115. *Id*.
116. *Id*.
117. *Id*.
118. *Id*. at 512.

The authors also discuss the challenge of regulatory oversight by detailing the origins of the OCC's "Fintech Charter Decision"; the tensions accompanying it;[119] its unique design;[120] the federal laws, rules, regulations to which it is subject;[121] and the authors' concern that the Fintech Charter Decision "severely restricts state financial services regulators' oversight."[122] The authors conclude that the Fintech Charter Decision imperils state regulatory agencies' oversight of predatory and unethical practices and hinders state regulators' ability to fund contemporary and future consumer protection enforcement efforts.[123]

The authors end by emphasizing the need for courts and regulators to weigh the advantages that fintech firms introduce with the strengths of historic banking platforms that provided a protective oversight role.[124] They also recommend formal rules that would restrict or, in some cases, completely ban regulators' reliance on algorithms in consumer credit markets.[125] In addition, the authors believe that explaining the programming behind AI models and applications could help resolve the issue of bias[126] and create a sense of trust between the algorithm and its user[127] as well as inform users about the system's flaws and how it should be properly operating.[128] If state and federal regulators work together to produce a uniform set of standards, they can reduce duplicate costs and conflicts[129] and provide enhanced oversight over potential biases and predatory targeting while also maintaining a balance between state and federal banking supervisors.[130] In essence, "thoughtful collaboration among state and federal regulators" could help construct "the best approach to achieve early and widely endorsed interventions that promote the accountability, transparency, and explainability" of learning algorithms.[131]

III. CONSUMER PRIVACY, ETHICAL DATA PRACTICES, AND THE IMPACT OF AI ON DEMOCRACY

The Symposium's final set of articles address data protection and collection issues. Modern AI relies on the collection of vast amounts of data. This information can provide us with conveniences and with initiatives like

119. *Id*.
120. *Id*. at 513 ("Banks that receive state charters are subject to the day-to-day supervision of state banking regulators but cannot evade federal regulation. Federal regulators supervise federally chartered banks and, to mitigate the challenges of complying with dual—and, at times, incongruent—regulatory obligations, federally chartered banks need only comply with limited state regulatory mandates."(footnote omitted)).
121. *Id*.
122. *Id*. at 519.
123. *Id*.
124. *See id*. at 505.
125. *Id*. at 522.
126. *See id*. at 523.
127. *Id*.
128. *Id*. at 524.
129. *Id*. at 525.
130. *Id*.
131. *Id*. at 529.

"smart cities" offering to use AI as a means to make life easier. At the same time, people's data can be put at risk. For example, consider AI programs that use patient medical information to make decisions—these offer new avenues of vulnerability. There can, however, be a lack of clarity by regulators and lawmakers regarding how seriously AI can implicate these concerns. Data regulation can exist as a patchwork that can quickly be rendered obsolete as technology progresses.

Regulators and governmental agents thus partner with the private sector to implement promising AI-centric initiatives. Sometimes, however, this relationship can result in the private sector assuming a sort of custodianship over traditionally "public" activities, like distributing public resources or protecting free speech. This circumstance begs the question: what are the implications on our society of relying so heavily on automated decision-making?

In their article, Ellen P. Goodman and Julia Powles examine the 2017 creation of the first model smart city in Toronto, Canada by Google affiliate Sidewalk Labs in partnership with Waterfront Toronto, a public development agency designed to revitalize the city's waterfront area.[132] This partnership, as the authors note, spurred intense national and international discourse concerning "innovation, privatization, privacy, surveillance, control, and the future of cities and urban life."[133] The authors do not inherently oppose the technology as a means to achieve urban reform, but they are troubled by the dominance of a single company, Google, performing community functions and controlling public life on Toronto's eastern waterfront. The authors believe that requirements should have been put in place initially to allay these concerns, most particularly the overriding role of just one company.[134]

The authors begin with the backdrop of Sidewalk's hasty development and the opaque process through which the project was approved. The authors explain that the Board of Waterfront Toronto was provided just a few days to examine the agreements that would govern its relationship with Sidewalk prior to being pushed to approve it. Even though the project garnered substantial interest by the public and the media, especially regarding issues such as ownership and governance, many city officials remained unclear about its long-term impact.[135] Regardless of how Sidewalk develops over the ensuing years, this first stage illustrates the perils of rushing to create a "smart city." It also demonstrates the implications of a clash between one of the world's most influential companies and a small, but highly informed, group of citizens, journalists, and community-based associations.[136]

The authors detail the starting stages of Sidewalk, ranging from Waterfront Toronto's initial request for proposals in March 2017 to the revelation of the

132. Ellen P. Goodman & Julia Powles, *Urbanism Under Google: Lessons from Sidewalk Toronto*, 88 FORDHAM L. REV. 457, 458 (2019).
133. *Id*. at 459.
134. *Id*. at 498.
135. *Id*. at 466.
136. *Id*. at 460.

"Master Innovation and Development Plan" in spring 2019, all the while emphasizing the extraordinary secrecy and ambiguity that enveloped the process.[137] Ontario's auditor general would later conclude that the parties involved selected "Sidewalk precipitously without adequately consulting the appropriate governmental entities."[138] For example, while the parties involved publicly released a four-page summary of the 2017 "Framework Agreement" between Waterfront Toronto and Sidewalk, they kept confidential the full twenty-nine-page agreement in addition to a number of other agreements they entered into.[139] The secrecy concerning the Framework Agreement, though perhaps typical of the Silicon Valley private sector, fueled an outcry by members of the community as well as public officials,[140] especially given both the monetary and nonfinancial costs of the project.

The authors are particularly critical of Sidewalk's proposed "digital layer" that would merge together different aspects of urban life within a vision of the "city as platform."[141] Yet, for the public, this proposal had three major problems: "privatization, platformization, and domination."[142] Sidewalk's "digital layer" promised robust data collection mechanisms that would, in turn, allow applications to autonomously deliver public services to citizens.[143] At the same time, Sidewalk's pervasive digital design, through its reliance on vast data flows and automated decision-making, would allow the company to control the activities that occurred over its network.[144] Because Sidewalk's vision is inexact, it hinders the ability of citizens to question its construction or to suggest methods of accountability.[145] Likewise, Sidewalk's depiction of "urban data" would make it so that "all places [would] become exposed and marketized."[146]

The authors make clear that their critique is neither aimed at technological advances nor urban innovation but rather at the enormous control of Alphabet-Google via Sidewalk "over nearly every aspect of the future district."[147] The authors recommend procedures that could alleviate some of their criticisms, including impact assessments for all of the project's proposed services;[148] nonetheless, they also give the sense that such recommendations may be "too late" because they could inadvertently endorse the "structural compromises" that have already been made.[149] Instead, all cities, including Toronto, should seek urban innovation but also

137. *Id*.
138. *Id*. at 463.
139. *Id*. at 464.
140. *Id*.
141. *Id*. at 476.
142. *Id*.
143. *See id.* at 477.
144. *See id*. at 478–79.
145. *See id*. at 484–85.
146. *Id*. at 486.
147. *Id*. at 498.
148. *Id*.
149. *Id*.

avoid providing such a key role to just one company. In contrast, Sidewalk has introduced a "vision where its own upper hand in platform control, data governance, intellectual property, procurement, and access has at each turn an obvious and legitimate alternative: the hand of the city itself."[150]

David W. Opderbeck discusses another realm in which AI risks clashing with the public interest—health care. Specifically, AI is fueling an intersection between the pharmaceutical and medical device industries.[151] For example, the contributions of "big datasets and complex algorithms will integrate the development and delivery of small- and large-molecule drugs, genetic therapies, and medical devices tailored to specific user profiles and even to individual consumers, with dynamic, real-time updates and adjustments."[152] As a result, Opderbeck contends, the legal system will require revised regulatory models in light of the increasingly muted distinctions between software code, medical technology, and drugs.

Opderbeck supports his arguments by discussing the means by which AI might substantially alter the present legal and economic scheme in the United States for drugs, biologics, and medical devices.[153] The Federal Food, Drug, and Cosmetic Act, through the U.S. Food and Drug Administration (FDA), "governs the sale of prescription drugs." The FDA is also in charge of "regulating biologics and medical devices"[154]—a vast responsibility that ensures that a drug is safe, effective, and properly labeled before it is presented to the FDA's Center for Drug Evaluation and Research in a "New Drug Application."[155] Opderbeck also describes the discovery, developments, and preclinical and clinical research that is involved with the introduction of a new drug.[156]

More recently, scientists have begun examining "large-molecule biologic products" as well as genomics in contrast to more traditional small-molecule pharmaceutical drugs.[157] Most drugs currently approved to sell on the market, and which are most familiar to the public, are small-molecule drugs.[158] While large-molecule drugs face the same scrutiny and approval process as their small molecule counterparts, they are substantially more complex and more difficult to assess for use on humans.[159] In contrast, there

150. *Id*.
151. David W. Opderbeck, *Artificial Intelligence in Pharmaceuticals, Biologics, and Medical Devices: Present and Future Regulatory Models*, 88 FORDHAM L. REV. 553, 553 (2019).
152. *Id*.
153. *Id*. at 554.
154. *Id*.
155. *Id*. at 555.
156. *See id*.
157. *See id*. at 557. "Large-molecule or 'biologic' drugs are made of proteins, usually copied or modified from existing human proteins," which "can be engineered to bind selectively to diseased cells, such as cancer cells." *Id*.
158. *See id*.
159. *Id*.

is currently no approval process for genetic therapies, another class of drug treatment, in the United States, and they are still considered experimental.[160]

Medical devices are subject to a different approval process altogether. They are classified according to three different levels of safety and effectiveness,[161] and the approval process differs according to the device's class.[162] Opderbeck claims that AI will likely upend these regulatory processes[163] by enhancing substantially the rate of standard biochemical and genetic research and decreasing the time, cost, error, and ethical challenges associated with human trials by relying on "in silico modeling" (i.e., computer simulations).[164]

While some AI devices are already being applied for these purposes,[165] challenges remain before these advances can go further.[166] Opderbeck is optimistic about how quickly AI will advance future research, ranging from reducing the costs of new drugs[167] to helping to customize individualized drug treatments or implants, to producing "highly customizable genetic therapies applicable only to a small population, perhaps even to specific individuals who could afford them."[168] Yet each new advance in AI in this field unearths the ethical challenges concerning "accountability, equity, and privacy."[169]

Opderbeck also discusses in detail new procedures currently being developed at the FDA for AI-driven in silico trials and medical devices as well as investigations into how AI may affect those procedures in the ensuing decades.[170] He observes that, although the "FDA is ahead of the game in creating guidance relating to AI and medical devices" and "seems to be behind concerning drugs, biologics, and genetic therapies,"[171] medical devices entail fewer public health risks. That said, he urges further regulatory development in privacy and security for medical devices,[172] noting that the FDA has failed to provide guidance on privacy.[173] Similarly, Opderbeck argues that the FDA should offer counsel regarding virtual patient models for in silico trials,[174] while noting the potential downside of working with private companies[175] and recommending that virtual patient models be placed into an open-source repository as one solution.[176]

---

160. *Id*. at 559.
161. *See id*.
162. *See id*.
163. *See id*. at 565.
164. *Id*. at 566.
165. *See id*.
166. *See id*. at 568.
167. *Id*.
168. *Id*.
169. *Id*. at 570.
170. *See generally id*.
171. *Id*. at 575.
172. *Id*. at 576.
173. *Id*.
174. *See id*. at 578.
175. *Id*. at 579.
176. *See id*. at 580.

With growing advances in AI technology, the FDA may need to develop new regulatory categories as well as greater privacy, accountability,[177] and modifications in intellectual property paradigms.[178] In addition, AI spurs topics such as concerns over global equity[179] as well as discussions about AI in drug and medical device production at the international level.[180] Toward these ends, Opderbeck contributes recommendations. First, he suggests that the FDA should provide clear privacy guidelines relating to AI and medical devices and trials, with the long-term goal of adopting a comprehensive, cross-sector data protection regime that is specifically tailored for AI.[181] In addition, Congress can revise regulatory models to accommodate the changes in intellectual property, privacy, and accountability that AI will bring.[182] As Opderbeck concludes, by 2050, "advances in AI could herald a new era in which goals of distributive justice relating to global public health could be more fully realized" and that advancements require "a new international AI treaty regime that accounts for public health values."[183]

Goodman and Powell's article on the Sidewalk Labs story and Opderbeck's article on the challenges impacting the FDA both demonstrate the practical and regulatory hurdles facing the proliferation of AI. As a data-intensive system, AI necessarily implicates data protection, cybersecurity, and user privacy issues. As both articles demonstrate, however, there can be a lack of clarity or true appreciation among regulatory governmental bodies about the scope of these issues. As a consequence, private sector entities, whether they be Google or medical device manufacturers, can exert influence over the public interest. However, the role of public interest custodianship can be at odds with private sector commercial interests and norms.

This trend is also apparent when dealing with the internet and social networking. The article by Madeline Byrd and Katherine J. Strandburg examines section 230 of the Communications Decency Act ("CDA 230"), which the authors contend gives "providers and users of 'interactive computer services' sweeping exemption from liability for actionable content created or published by others."[184] CDA 230, while often credited as "the law that gave us the modern internet,"[185] has spurred heated debated from those who claim that the Act has filled the internet with inaccurate and

177. *See id*. at 582.
178. *See id*. at 583.
179. *Id*. at 587.
180. *Id*. at 587–89.
181. *See id*. at 589.
182. *Id*.
183. *Id*.
184. Madeline Byrd & Katherine J. Strandburg, *CDA 230 for a Smart Internet*, 88 FORDHAM L. REV. 405, 406 (2019). "Its central provision states: '[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.'" *Id*. (quoting 47 U.S.C. § 230(c) (2012)).
185. *Id*. at 405 (quoting Derek Khanna, *The Law That Gave Us the Modern Internet—and the Campaign to Kill It*, ATLANTIC (Sept. 12, 2013), https://www.theatlantic.com/business/archive/2013/09/the-law-that-gave-us-the-modern-internet-and-the-campaign-to-killit/279588 [https://perma.cc/3FNB-2UJ3]).

distorted information that is biased against women and minority groups.[186] The authors focus on CDA 230 liability with respect to the increasing use of "smart services," which tailor content based on models and predictive data on individual users. They also use, as a case study, recent legal challenges to Facebook's ad-targeting platform.[187]

The authors provide support for their viewpoints by outlining CDA 230's background and the relevant case law in terms of "a secondary liability frame."[188] They emphasize that, in 1996, Congress expected that if online service providers were removed from liability, the providers would offer technological methods to resolve the content-screening challenges.[189] Today, however, the authors contend that there is far too much user-generated content to effectively screen for actionable defamatory, harassing, or offensive conduct.[190] The drafters of CDA 230 greatly miscalculated the potential form and volume of offensive content and "would have been horrified by the tsunami of racist, sexist, homophobic, fraudulent, untruthful, and otherwise hurtful discourse that has accompanied the internet's benefits."[191]

As the authors explain, under CDA 230 a defendant is protected if they are categorized as a publisher of information given by another content provider.[192] Yet because CDA 230 does not define "publisher," courts have experienced difficulty in interpreting the term's meaning.[193] In turn, earlier cases shielded "service providers against both 'publisher' and 'distributor' liability."[194] Such shielding has encouraged courts to interpret CDA 230 broadly.[195]

That said, CDA 230 does define an "'information content provider' as 'any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.'"[196] Accordingly, courts have "routinely treated service providers as potentially liable 'information content providers' when they or their employees independently created or developed actionable content" (that is, courts have denied immunity under these circumstances); but courts have consistently granted immunity "when plaintiffs alleged merely that a provider knew that a service was being used for illegal purposes or profited from a third party's creation and publication of actionable content."[197] Between these two extremes, however, there exist intermediate cases in which courts will granted or denied immunity based on the degree

186. *Id*.
187. *Id*. at 406.
188. *Id*.
189. *Id*. at 407.
190. *See id.*
191. *Id*.
192. *Id*. at 408.
193. *Id*.
194. *Id*.
195. *Id*. at 409.
196. *Id*. at 410 (quoting 47 U.S.C. § 230(f)(3) (2012)).
197. *Id*.

to which the service provider can be said to have "developed" the content in question.[198] This distinction, however, is not a bright-line analysis.[199]

The authors also explain Facebook's ad-targeting platform, which uses automated processes to select an audience for certain advertisements based on users' site activity and some offline data sources.[200] This methodology can, according to empirical research, produce biased targeting[201] and demographic disparities in the base audience.[202] As a result, the National Fair Housing Alliance filed a class action lawsuit which, in March 2019, settled with a consent decree that "requires Facebook to limit the ways in which the tools . . . can be used for targeting housing, employment, or credit" advertisements.[203] Facebook will make these changes "[o]n or before September 30, 2019," using a tool called HEC Flow, which will change the audience selection tools in a number of ways.[204]

As a way of providing a foundational background, the authors elucidate the principles of discriminatory advertising law under the Fair Housing Act (FHA) and discuss the potential liability for Facebook's audience selection tools.[205] Assuming Facebook's ad-targeting platform has incurred liability for actionable discrimination, the authors then assess Facebook's liability for failure to correct under 24 C.F.R. 100.7(a)(iii)[206] and contend that the company could be liable.[207] A court could find that Facebook should be liable for "failure to correct" discriminatory attribute-based targeting as well as the disparities which resulted from its lookalike audiences tool.[208] The authors then use a parallel type of analysis in examining CDA 230's applicability to Facebook's audience selection tools,[209] emphasizing that courts "are thus likely to conclude that ad targeting is at least generally a 'publisher' activity and to reject plaintiffs' arguments that 'failure to correct' claims in particular are beyond the scope of CDA 230."[210]

Byrd and Strandburg also examine CDA 230 from a secondary liability perspective,[211] noting that CDA 230 most likely does protect Facebook from the FHA's effectively secondary "failure to correct" liability and emphasizing that "allegations of discriminatory ad targeting have nothing to do with content development." In short, "CDA 230 was simply not designed or intended to handle situations in which a service provider's *activities* as a

198. *See id.* at 410–11.
199. *See id.* at 410.
200. *Id*. at 412.
201. *Id*. at 413.
202. *Id*. at 413–14.
203. *Id*. at 414.
204. *See id*.
205. *Id*. at 415.
206. *See id*. at 416.
207. *See id*. at 419–25.
208. *See id*. at 422–24.
209. *Id*. at 425–29.
210. *Id*. at 426.
211. *Id*. at 429.

publisher are actionable but the published *content* is not."[212] While courts have attempted to discover approaches for applying CDA 230 to smart online service providers, they have faced challenges because the definition of "information content provider" is the only relevant provision.[213]

In acknowledging the limits of CDA 230,[214] the authors offer recommendations. First, they suggest amending CDA 230 "to clarify that a party is not 'treated as the publisher or speaker of any information provided by another information content provider' unless liability is premised primarily on the actionable nature of that third-party content."[215] They also propose "adding a provision to CDA 230 conferring immunity on providers of online services capable of substantial nonactionable uses when two conditions are satisfied: (1) liability is based on the design of the service; and (2) the service cannot reasonably be designed to avoid liability while retaining substantial nonactionable uses."[216] Lastly, they propose ensuring that "[s]econdary liability provisions based on a defendant's contribution to, facilitation of, or failure to monitor actionable user behavior would be preempted and replaced by a contributory liability regime combining a 'material contribution' requirement with a 'knew or should have known' mental state"; immunizing online service providers "from substantive inducement liability regimes, unless and until regulators redesigned or reaffirmed their applicability" to online service providers; and applying these rules "to both federal and state statutes and regulations."[217]

Facebook's advertising platform is an oft-cited example of a potential pitfall of automated decision-making. Yet, as Ari Waldman contends in the final essay of this section, widespread proliferation of AI risks undermining principles of accountability across many different aspects of society. Waldman notes that automated decision-making systems that rely on "'big data'–powered algorithms" and machine learning are just as likely to commit error and hold biases as humans.[218] As the previous authors to this issue have demonstrated in their discussions of Google and Facebook, the lack of transparency surrounding the technology magnifies these concerns.[219]

Whether these features should eliminate algorithmic decision-making altogether as any source of authority is a reasonable question[220] given that automating decisions about commercial and societal products may contravene the kinds of democratic safeguards that we cherish, most particularly equality and fairness.[221] Yet some scholars also suggest that there are procedures that can curtail the biases so that that they no longer pose

212. *Id*. at 434.
213. *Id*.
214. *Id*. at 434–36.
215. *Id*. at 436.
216. *Id*. at 436–37.
217. *Id*. at 437–38.
218. Ari Ezra Waldman, *Power, Process, and Automated Decision-Making*, 88 FORDHAM L. REV. 613, 614 (2019).
219. *Id.*
220. *Id*. at 615.
221. *Id*.

risks.[222] Similarly, Waldman believes that society should impose mandates that all automated decision-making entities, both governmental and private, should obey.[223]

Waldman supports his argument by first setting out and criticizing the parameters of algorithmic systems and why they are both so attractive as well as dangerous in a society that values democracy.[224] For example, while automated decision-making systems have powerful predictive abilities based on existing data,[225] they can also make serious mistakes that can have real world impact[226] as well as draw into question the fairness of such systems.[227] Likewise, the more accurate such systems become, the more complex and vague they appear to those trying to decipher their biases[228] or take back control.[229] These circumstances shift the decision-making power from humans to technology[230] and potentially undermine the legitimacy of law.[231] Indeed, not only can algorithms inject racial, gender, and socioeconomic biases into a culture[232] but the biased data sets that feed them "can entrench second-class citizenship for marginalized populations."[233]

By reviewing existing proposals to limit algorithmic decision-making and expand accountability, Waldman creates a substantive approach[234] that includes "impact assessments, source code transparency, explanations of either the result or the logic behind it, and a human in the loop who can hear someone's appeal."[235] While these suggestions are appealing, however, Waldman does not believe they can close the gaps "in the underlying social and political system that not only lays the groundwork for algorithmic decision-making but sees its proliferation, despite its biases, errors, and harms, as a good thing."[236] In short, the efficiency aspect of algorithmic decision-making can favor machines over humans[237] and is therefore "presumptively illegitimate until it can be shown to reflect more than just neoliberal values of innovation and efficiency."[238]

In particular, algorithmic decision-making can embolden engineers to make policy decisions, therefore reinforcing their devotion to efficiency over any concern regarding privacy or other community values.[239] In turn, the

222. *Id*.
223. *Id*. at 616.
224. *Id*. at 617.
225. *Id*. at 618.
226. *Id*.
227. *Id*.
228. *Id*. at 618–19.
229. *Id*. at 619.
230. *Id*. at 620.
231. *Id*.
232. *Id*. at 621–22.
233. *Id*. at 622.
234. *Id*.
235. *Id*. at 624.
236. *Id*.
237. *Id*. at 625.
238. *Id*. at 624.
239. *Id*. at 626.

tenets of neoliberalism[240] show how accountability for the results of algorithmic decision-making can be "recast as compliance,"[241] an alteration that not only invites corporate interests but threatens social standards.[242]

Waldman believes that, in order to make algorithmic systems fulfill basic social values other than efficiency, regulators must independently evaluate the "code of automated systems for noncompliance with values like equality, nondiscrimination, dignity, privacy, and human rights"—an approach that academic researchers have been successfully following.[243] In addition, each level of federal and state government "could enact legislation that expresses the values society wants algorithmic decisions to reflect" and therefore construct "socially conscious algorithmic decision-making systems."[244]

Because "algorithmic decision-making is a product of the neoliberal managerial project,"[245] Waldman contends it needs strict oversight, most particularly by regulators and "independent academic experts" who can inspect the system code to ensure that it is abiding by our normative principles.[246] Those devices that fail to pass these kinds of independent tests should not be released or used.[247] As Waldman concludes, this type of strategy has two research requirements: first, the use of sophisticated research to create procedures "for interrogating decision-making code" and, second, the application of legal policy research to best assemble a regulatory body that can make certain that algorithmic decision-making systems continue to reflect the values we cherish as a society.[248]

CONCLUSION

AI and robotics are fast-moving fields, with new developments happening seemingly every day. Though no one knows exactly what the future holds for these technologies, we hope this Symposium marks the beginning of an ongoing discussion between the different professions. The onus is on us to determine what we make of technology. Will it mark the beginning of a new golden age for humanity or will it spiral us into a dystopian nightmare? Will we be *Tomorrowland* or *The Terminator*?

240. According to Waldman, "Neoliberalism is a political philosophy that aims to replace and undermine a political system based on social justice and social welfare with a regime that is 'characterized by private property rights, individual liberty, unencumbered markets, and free trade.'" *Id.* at 625 (quoting David Harvey, *Neoliberalism as Creative Destruction*, 610 ANNALS AM. ACAD. POL. & SOC. SCI. 22, 22 (2007)).

241. *Id.* at 628.

242. *Id*. at 628–29.

243. *Id*. at 630.

244. *Id*. at 631.

245. *Id*.

246. *Id.*

247. *Id*.

248. *Id*. at 632.