

FUTURE-PROOFING ROBOTICS: LIMITING MANUFACTURER LIABILITY FROM AUTONOMOUS PROCESSES

Ryan Whittington

I. INTRODUCTION

The law of torts is not concerned with perfection. Humans are fallible and tort law serves as a reflection of humanity's shortcomings. While tort law does not require perfection, it does require that individuals do their part to avoid harming one another. As such, individuals are expected to comport themselves in a reasonable manner and avoid causing harms which are reasonably foreseeable. The robotics industry may challenge some of the premises underlying the law of torts.

The ever-growing presence of sophisticated robots in the stream of commerce presents a number of challenges to our existing, human-centric approach to tort law. First, the growing prevalence of robots in the field will offload a substantial share of risk from consumers onto producers. Second, the concept of emergence (or autonomy), defined as "unpredictably useful behavior" exhibited by robots,¹ sits in tension with tort law principles like foreseeability and control.

In light of such tension, lawmakers may need to create a new framework for assigning liability. Looking forward, we must ask whether our existing tort framework is sufficient to meet the challenges of the future. In other words, we must ask whether or not sophisticated robots should be treated as exceptional under the law. Ultimately, society's desire for innovation and the continued development of the robotics industry may necessitate the establishment of a framework that shifts liability away from the manufacturers of emergent robots.

II. ASSIGNING LIABILITY IN A ROBOTIC FUTURE

The ever-increasing introduction of robots into the stream of commerce may dramatically alter the balance of liability between consumers and producers. As a threshold matter, rather than dedicate significant space to developing a precise definition for the term "robot," this paper will rely on Ryan Calo's definition. Robots

¹ Ryan Calo, *Robotics and the Lessons of Cyber Law*, 103 CAL. L. REV. 513, 532 (2015). Available at: <http://scholarship.law.berkeley.edu/californiareview/vol103/iss3/2>.

can be defined as “artificial objects or systems that sense, process, and act upon the world” and have three “essential qualities—embodiment, emergence, and social valence.”²

Though we are far removed from the point in which robots match the generalized depth and complexity of human intelligence, robots are poised to outmatch humans in a variety of discrete capacities.³ In a particularly high profile case, IBM’s Watson, a computer system that leverages natural language processing and machine learning to answer questions, was victorious in a game of Jeopardy against prodigious Jeopardy Champions Brad Rutter and Ken Jennings.⁴ Since the 2011 match, sophisticated machines have continued to make exceptional strides.

As robots become increasingly capable of accomplishing human tasks, there will almost certainly be pressure to put these machines into the field. Driven by an urge to promote public safety and reduce public harm, these machines will be put into the field. Take autonomous vehicles, for instance. Over 90% of automobile collisions result from human error.⁵ Given this figure, along with the staggering number of fatalities caused by automobile accidents each year, there will be immense pressure aimed at getting autonomous vehicles onto the road and human drivers off of the road. Robots will continue to exceed the capacity of humans in a growing number of fields and as a result, it will be a moral imperative to deploy these machines.⁶

As more sophisticated robots are introduced into the stream of commerce and as more individuals offload labor onto these machines, the balance of risk between consumers and producers will dramatically change.⁷ Assigning risk in this commercial future will

² *Supra* note 1.

³ Emerging Technology from the arXiv, *Experts Predict When Artificial Intelligence Will Exceed Human Performance*, MIT TECHNOLOGY REVIEW (May 31, 2017) <https://www.technologyreview.com/s/607970/experts-predict-when-artificial-intelligence-will-exceed-human-performance/>.

⁴ John Markoff, *Computer Wins on ‘Jeopardy!’: Trivial, It’s Not*, NEW YORK TIMES (Feb. 16, 2011), <https://www.nytimes.com/2011/02/17/science/17jeopardy-watson.html?mtref=www.google.com&gwh=0C63F63801DAF832C547FC0994645BDC&gwt=pay>.

⁵ *Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey*, NHTSA (Feb. 2015), <https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812115>.

⁶ Jason Millar & Ian Kerr, *Delegation, Relinquishment, and Responsibility: The Prospect of Expert Robots*, SSRN (Mar. 18, 2013), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2234645.

⁷ F. Patrick Hubbard, “*Sophisticated Robots*”: *Balancing Liability, Regulation, and Innovation*, 66 FLA. L. REV. 1803, 1859 (2015).

largely depend on the degree of control consumers manage to maintain over their machines. But as robots become more sophisticated and continue to substitute for human labor and control, the prevailing framework for assigning liability will be challenged.

Liability will be particularly difficult to assess in cases in which robots demonstrate “emergent” behavior. Emergence can be defined as the “unpredictably useful behavior” of robots.⁸ The development of emergent machines is “a clearly stated goal of robotics and artificial intelligence.”⁹ In emergent systems, robot producers are less concerned with training machines; rather than “designate every behavior with its own block of code, users can set goals and train the system to accomplish them.”¹⁰ Perhaps most significantly, emergent behavior can lead to the development of machine-created solutions that “no human would have come to on her own.”¹¹

In terms of product quality and innovation, emergence is undoubtedly important. However, the concept of emergence challenges existing methodology for assigning liability. Emergent behavior is inherently unpredictable; as stated above, programs demonstrating emergence are capable of coming up with solutions that no human would have come up with. This unpredictability sits uncomfortably in direct tension with applications of tort law that treat foreseeability and control as central precepts.¹²

III. PRESERVING DYNAMISM IN A WORLD OF EMERGENT ROBOTS: SAFE HARBOR FOR MANUFACTURERS?

The prospect of emergent robots places manufacturers and designers at risk. Given the unpredictability inherent to emergent processes, manufacturers may not be able to reasonably foresee the risks of harm associated with emergent behavior. Moving forward, lawmakers should assess the relationship between legal risk and commercial development and determine whether or not our current approach to liability is sufficient to meet the challenges of the future. Lawmakers must ask whether the often unforeseeable legal risks associated with emergent robots should be borne entirely by producers. In light of such risks, lawmakers should consider extending safe harbor protections to robot manufacturers, effectively shielding these producers from liability in cases in which sophisticated robots cause harm as a result of emergent processes.

⁸ *Supra* note 1 at 532.

⁹ *Id.* at 537

¹⁰ *Id.* at 538

¹¹ *Id.* at 539

¹² Further applications of this can idea are described in Section V.

In doing so, lawmakers should look to the early development of cyber law and the example of Section 230 of the Communications Decency Act as a possible template.

A. Lessons from Cyberlaw:

The question posed to lawmakers now is similar to the question undergirding much of tort law: How do we balance our desire to minimize harm without overburdening the productivity of society? Lawmakers had to answer such a question in the 1990s in response to another emerging technology. In 1996, Congress passed the Communications Decency Act (CDA). While many provisions were ultimately struck down as unconstitutional, Section 230 of the bill remains as a vital foundation of internet law.¹³

Section 230 applies to “interactive computer services” and offers these services legal protections in the face of legal uncertainty.¹⁴ The first prong holds that no provider of an “interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider”; the second prong holds that interactive services will not be held liable for “any action voluntarily taken in good faith to restrict access” to content.¹⁵ In the words of Section 230’s original sponsor in the House of Representatives, now-Senator Ron Wyden, the two prongs of Section 230 can be thought of as a “shield and a sword.”¹⁶ The law “shields” platforms from vicarious liability stemming from the conduct of their third party users. The law grants platforms a “sword” in the sense that it grants platforms with the ability to take moderation actions without being deemed a publisher.

The text of Section 230 sheds light upon the purpose of the statute. One of the major purposes was to promote free expression. The law states specifically that “a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.” In other words, Section 230 was concerned with the prospect of platforms burdening more speech than necessary. Absent Section 230 protection, platforms would likely over-police their forums in an effort to minimize legal risk. But in addition to the legislation’s free speech

¹³ *Supreme Court Rules CDA Unconstitutional*, CNN (June 27, 1997), <http://www.cnn.com/US/9706/26/cda.overturned.hfr/>.

¹⁴ 47 U.S.C. § 230

¹⁵ *Id.*

¹⁶ Colin Lecher, *Sen. Ron Wyden on Breaking Up Facebook, Net Neutrality, and the Law That Built the Internet*, THE VERGE (Jul. 24, 2018), <https://www.theverge.com/2018/7/24/17606974/oregon-senator-ron-wyden-interview-internet-section-230-net-neutrality>.

aims, Section 230 explicitly seeks to protect online platforms from liability with the intention of promoting the commercial development of the internet. According to Section 230's text, the legislation is designed to "promote the continued development of the Internet," "preserve the vibrant and competitive free market," and ensure the Internet remains "unfettered by Federal or State regulation."¹⁷

Though online platforms are different from emergent robots in a significant number of ways, the robotics industry has a similar set of considerations. Like the platform economy absent Section 230, robotics manufacturers are subjected to an unpredictable legal environment that has the potential to hinder commercial development.¹⁸ Regarding platforms, Congress sought to address the problem of unpredictability in order to promote the cause of commercial viability.¹⁹ In other words, prior to the passage of Section 230, Congress had failed to create a public policy environment in which online platforms and other intermediaries could really flourish on the internet.

Similarly, today and in the future, manufacturing emergent robots will effectively open manufacturers up to unreasonable and unforeseeable legal risks.²⁰ Firms will likely take such legal risk to heart. If legal risks associated with the unpredictability of robots are not addressed through public policy, there is a possibility that the commercial development of the robotics industry may falter. One way to address the legal risks associated with unpredictability would be to take inspiration from Section 230 and create public policy that effectively grants safe harbor to the manufacturers, designers, and developers of emergent robots.

What would such a policy look like? Such a policy should effectively port over applicable language from Section 230. While the law's provisions dealing with content moderation do not meaningfully port over between industries, 47 U.S.C. § 230(c)(1) can be applied to the field of robotics with a couple of modest changes. This subsection outlines the extent of protection extended to online platforms: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any

¹⁷ 47 U.S.C. § 230

¹⁸ Ryan Calo's argument in favor of safe harbor for the creator of robotics platforms outlines the need for certain forms of immunity in order to promote the expansion of robotics. Ryan Calo, *Open Robotics*, 70 Md. L. Rev. 571 (2011).

¹⁹ *Supra* note 22

²⁰ Matthew U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, 29 Harv. J. L. & Tech. 354

information provided by another information content provider.”²¹ This language could easily be modified in a new piece of legislation to reflect the reality of the robotics industry. By replacing “interactive computer services” with “manufacturers of robotic machines demonstrating emergent properties,” Congress could create a statutory framework that promotes commercial innovation and provides certainty to manufacturers that their creations won’t expose them to unreasonable legal risk.

B. Differences in Harm—Comparing Physical and Cyber Spaces

The benefits of safe harbor for robot manufacturers are clear. Extending Section 230-style safe harbor provisions to producers would ensure that manufacturers can be held liable only for foreseeable harms. While a Section 230-style approach to emergent robots might grant manufacturers, designers, and developers the breathing room necessary to usher in future innovations, there are a handful of significant consequences that might stem from such a policy:

First, analogizing between online intermediaries may be futile given the corresponding scopes of harm. Commercially, there are number of legal risks associated with operating internet platforms and creating autonomous robots. However, the scope of harm between these two types of operations is ordinarily different. The risks associated with operating a platform are largely non-physical. Emergent robots, however, must deal with the added complexities of “embodiment.” Robots are “embodied” in the sense that they are “sensing, navigating, and acting upon the world...which generally requires a physical presence.”²² Because of this embodiment, emergent robots are distinct from software and online applications in the sense that the ability to interact with the physical world often “translates, in turn, to the potential to physically harm people or property.”²³ Given that harm in physical space often manifests as bodily harm or property damage while harm in cyberspace often manifests as dignitary harms like defamation these worlds may simply be too different to compare.

But while the physicality of harm stemming from emergent robots may be a considerable distinction between emergent robots and online platforms, the presence of physical harm alone should not be sufficient to rule out applying Section 230 principles to the

²¹ 47 U.S.C. § 230(c)(1)

²² *Supra* note 1.

²³ *Id.*

field of robotics. In fact, Section 230 has been interpreted to apply to certain physical harms as well.²⁴ For instance, In *Inman v. Technicolor USA, Inc.*, a plaintiff contracted mercury poisoning after purchasing vacuum tubes from a third party seller on eBay. In this case, eBay was found to be immune from liability under Section 230.²⁵ Additionally, the case of *Doe v. MySpace, Inc.*, is instructive. In *MySpace*, an individual assaulted a minor that he met on the MySpace social media platform.²⁶ Following the incident, the victim brought a negligence suit against MySpace. The Fifth Circuit ultimately ruled that the platform was, indeed, protected from liability by Section 230. The physical harms resulting from the two causes of action were not deemed reasonably foreseeable. Though the harms generated by robots are more likely to be physical in nature, the mere existence of physical harm alone is not sufficient to challenge the comparison between platforms and robots.

C. *Where, If Anywhere, Should Liability Exist?*

A second potential consequence of tailoring safe harbor protections for the manufacturers of emergent robots is that such an arrangement might deprive individuals that suffer harm of the opportunity to seek remediation through the law of torts. In certain cases, the emergent behavior or the creative conduct of a machine or program may be so unforeseeable that it would not make sense to hold producers liable. Safe harbor protection would effectively codify this immunity from liability. But if individuals that have suffered harm at the hands of autonomous processes are not able to file suit against manufacturers, designers, or developers, then who may they challenge? Given tort law's interest in compensating the victims of harm, it is critical that we take this question seriously.

The answer that would be most satisfactory to plaintiffs is, unfortunately, will not likely be viable in the near future. The most efficient outcome would be to protect producers from the actions of programs outside the realm of foreseeability and offload this risk onto the agent responsible for actually causing the harm. Unfortunately, in such cases, the responsible agent would be a non-sentient robot. Given that robots generally do not have money or a way to make victims whole, the idea of assigning liability to non-sentient robots is likely a non-starter. Inability to assign liability to the autonomous machines that generate harm, however, does not

²⁴ Danielle Keats Citron & Benjamin Wittes, *The Problem Isn't Just Backpage: Revising Section 230 Immunity*, 2 *Geo. L. Tech. Rev.* 453, 464 (2018).

²⁵ *Inman v. Technicolor USA, Inc.*, Civil Action No. 11-666, 2011 WL 5829024 (W.D. Pa. Nov. 18, 2011).

²⁶ *Doe v. MySpace, Inc.*, 528 F.3d 413 (5th Cir. 2008).

mean manufacturers should be required to bear the burden of unforeseeable outcomes.

Even if individuals cannot successfully bring suits against either unruly robots or their manufacturers, victims may still be able to successfully bring cases against individuals that place robots into the field and maintain control over the products. In other words, victims can seek damages from individuals under no-fault tort doctrines rooted in the control of an agent. Presumably in many cases, robots effectively act as agents of the individuals who place them in the field. The doctrine of respondeat superior is based on the idea that “fairness requires that an employer, who benefits from being able to control an employee’s conduct in the pursuit of the employer’s business, be liable for the torts committed by the employee.”²⁷ This doctrine could be revised to instead reflect the owner-robot relationship, in which a human individual is the beneficiary of the robot’s labor. Additionally, tort doctrines governing human control over children and animals could provide victims with alternative avenues for remediation.²⁸ While these doctrinal approaches to vicarious liability may provide victims avenues to seek damages, admittedly, none of these doctrines is a perfect fit. Though it will be difficult to assign liability when robots cause harm through their emergent properties, we should nonetheless avoid offloading all risk from emergence onto robot manufacturers.

Section 230 has ushered in similarly vexing questions pertaining to the assignment of liability. The architecture of the Internet makes it particularly difficult to identify and authenticate users’ identities.²⁹ As such, the Internet has a tendency towards anonymity. This can make it incredibly difficult for victims to seek damages when they believe they have been the victim of tortious conduct. In cases in which an individual has been defamed or otherwise harmed by an anonymous user online, the victim effectively has no means of seeking damages. Internet services that provide platforms to anonymous users are shielded from liability under Section 230 and, because the Internet makes anonymity easy, the perpetrator of the harm will likely be unknown.³⁰

²⁷ *Supra* note 13 at 1863.

²⁸ *Id.*

²⁹ See LAWRENCE LESSIG, CODE VERSION 2.0 (2006).

³⁰ A recent lawsuit illustrates this concept. Author Stephen Elliott is suing Moira Donegan, the journalist who created the “Shitty Media Men” list, for defamation. This list was an editable Google spreadsheet that journalists circulated among their peers; recipients of the list were invited and encouraged to “share their experiences with men identified on the list.” Stephen Elliott was

As a closing note, it should be noted that the creation of tailored safe harbor protections does not mean that firms will inevitably shirk the task of mitigating all harm. In the world of Section 230, regardless of liability protections, platforms have an incentive to police content on their platforms. While Section 230 grants platforms a strong affirmative defense against certain claims, Section 230 defenses often fail and legal challenges still require platforms to engage in lengthy and expensive litigation.³¹ This will also be the case with emergent robots. Even if safe harbor protections are extended to protect manufacturers, such protections will only apply when machines act beyond their foreseeable protocols. Further, litigation pertaining to robotic emergence will be complex and expensive. Manufacturers of robots have incentives to reduce harm wherever possible.

IV. CONCLUSION

Though there are substantial differences between the platform economy and emergent robots, the industries have some critical similarities. For one, both robots and information platforms are operating in spaces that carry substantial legal risks absent statutory protection. Because people are often careless, ignorant, and mendacious, it is inherently risky to operate a platform that invites third party users to participate. Similarly, it is inherently risky to create machines that will act in an inherently unforeseeable manner.

But despite the risks of harm associated with both industries, there are substantial reasons to support extending protection from liability. Both the commercial internet and the field of robotics are vital industries and policymakers should endeavor to develop a

among those identified on the list and was accused of committing sexual assault. In this case, Donegan is likely protected from the defamation claim under Section 230. Further, due to the anonymity afforded by Google's collaborative spreadsheet application, the individual(s) that posted the supposedly defamatory material are also protected. Taken together, Elliott feels he has been harmed by another's tortious conduct. However, Section 230 makes it particularly difficult for Elliott to seek damages as a plaintiff. See Aaron Mackey, *Lawsuit Seeking to Unmask Contributors to 'Shitty Media Men' List Would Violate Anonymous Speakers' First Amendment Rights*, EFF (Oct. 16, 2018), <https://www.eff.org/deeplinks/2018/10/lawsuit-seeking-unmask-contributors-shitty-media-men-list-would-violate-anonymous>; see also, Christina Cauterucci, *Does Stephen Elliott's Lawsuit Against Moira Donegan Have a Chance to Succeed?*, SLATE (Oct. 12, 2018), <https://slate.com/news-and-politics/2018/10/stephen-elliott-moira-donegan-lawsuit-analysis.html>.

³¹ Section 230 defenses failed "a third of the time," and "even when it proved a successful defense, a year had often passed in the interim." *Supra* note 22 at 655.

policy framework that encourages continued innovation in these spaces. Section 230 helped ensure that the open internet could be a viable commercial enterprise. Since the law's introduction, the Internet has proven to be a transformative technology. In looking to the future, lawmakers should create a legal framework around robotics that ensures the robotics industry is able to meaningfully develop. By protecting manufacturers from the legal risks associated with unforeseeable harms, lawmakers can prepare the robotics industry for the future.