Outsmarting Smart Devices: Preparing for AI Liability Risks and Regulations

KATHRYN BOSMAN COTE*

TABLE OF CONTENTS

* © 2024 Kathryn Bosman Cote. J.D. Candidate 2024, University of San Diego School of Law; B.A. 2020, University of Southern California.

I. INTRODUCTION

Technology is advancing at a rapid rate, with 64 billion Internet of Things (IoT) smart devices expected to be in use as of 2025.[1] Although artificial intelligence ("AI") has been in use since the 1950s, recent technological advancements such as battery energy density and increased software capability have driven the mass adoption of AI across all consumer products.[2] Today, AI is found in "personal robots, children's toys, home appliances, virtual reality devices, and pool monitoring systems."[3] The rapid development and saturation of AI make it critical to settle issues of accountability and liability.[4] Specifically, it is important to examine the context in which a machine can be held responsible for its actions or sanctioned when it makes decisions for itself through machine learning.[5] For consumers to receive compensation, the critical issue of responsibility serves as a preventative tool that discourages companies from causing harm for which they could be held liable.[6] However, assigning responsibility, and therefore liability, to self-taught AI can be challenging when it is impossible "to know for certain who or what is responsible for [the] final decision" that caused harm or inflicted damages.[7]

What happens when a company creates an AI self-learning chatbot that makes decisions the company did not expect or evolves to make racist comments? That was the case for Microsoft with the launch of their AI chatbot "Tay," which was designed "to develop conversational understanding

1. U.S. CONSUMER PRODUCT SAFETY COMM'N, POTENTIAL HAZARDS ASSOCIATED WITH EMERGING TECHNOLOGIES 13 (Sept. 30, 2022) [hereinafter CPSC, *Potential Harms*].
2. *Id.* at 5
3. *Id.*
4. Kanicka Kalra, *The Future Is Now: Robots as Surgeons: The Adoption of Surgical Safety Standards to Robotic Surgery*, 2022 INT'L J. L. ETHICS TECH. 1, 1 (2022).
5. *Id.*
6. Jhanavi Gupta, *Artificial Intelligence in Legal System: An Overview*, 4 INT'L J.L. MGMT. & HUMAN. 6076, 6078 (2021).
7. Anat Lior, *The AI Accident Network: Artificial Intelligence Liability Meets Network Theory*, 95 TUL. L. REV. 1103, 1108 (2021); *see* Kalra, *supra* note 4, at 9 (who is responsible in the case "of misdiagnosis by the robotic surgeon" which causes harm to the patient); *see generally* Dongyun Zhu, *Research on Legal Risks and Legal Regulations of Autonomous Driving from the Perspective of Civil Law*, 108 J.L. POL'Y & GLOBALIZATION 18–19 (accountability when "the system developer is no longer alive," but the system is "constantly learning and changing").

by interacting with humans."[8] Within 24 hours of its launch, Twitter users "tricked the bot into posting" racist comments, ethnic slurs, and hate speech.[9] Who is responsible for the chatbot's actions? Is it Microsoft who created the AI with a deficiency in discriminatory and bias training, or is it the Twitter users who taught and manipulated the chatbot into making racist comments?

What about when a company creates a self-driving car that supposedly malfunctions and causes a crash? In December 2022, a Tesla Model S in "full self-driving mode" malfunctioned and caused an eight-vehicle crash.[10] Tesla had instructed drivers that the software was not autonomous and required "active driver supervision."[11] So, is it the driver's fault for not taking control over the car as instructed, or is it the car manufacturer's fault for creating the faulty software? Or should both parties be partially responsible?

Through examining the current strict liability regime for AI and analyzing potential benefits and drawbacks, as well as examining recent U.S. and EU regulatory and legislative guidance, this paper will propose a liability scheme to best fit the complexity of AI, as well as provide guidance to consumers, companies, and regulators on how to approach the rapidly evolving issue of AI and smart devices.

II. SETTING THE STAGE

A. What is AI/ML/IoT?

AI, IoT, ML – in the age of quickly evolving technology, the market is saturated with abbreviations. These abbreviations can obscure definitions and make it challenging for both consumers, practitioners, and companies to fully grasp what these terms mean and how they all interact with one another.

AI, or "artificial intelligence," is a system that takes in and processes large amounts of data and uses that data to "make autonomous decisions to achieve specific goals."[12] Many AI systems have the ability of ML, or

8. Amy Kraft, *Microsoft Shuts Down AI Chatbot After it Turned Into a Nazi,* CBS NEWS (Mar. 25, 2016, 7:53 PM), https://www.cbsnews.com/news/microsoft-shuts-down-ai-chatbot-after-it-turned-into-racist-nazi/ [https://perma.cc/7z38-SFDD].

9. *Id.*

10. Edward Helmore, *Tesla Behind Eight-Vehicle Crash Was in 'Full Self Driving' Mode, Says Driver,* THE GUARDIAN (Dec. 22, 2022), https://www.theguardian.com/technology/2022/dec/22/tesla-crash-full-self-driving-mode-san-francisco [https://perma.cc/2HAV-CP9M].

11. *Id.*

12. Felicia Johansson, Can Things be Defective Products? An Analysis of the Product Liability Directive Applied to IOT 20 (2021) (Master's Thesis, Lund University).

"machine learning," which is also known as the ability for "self-learning."[13] Certain AI systems have the capacity to identify patterns in data sets and past outcomes of previous processes and use those patterns to predict future outcomes.[14] Thus, these systems have the power to optimize over time.[15]

The Internet of Things "IoT" has emerged out of AI and "involves the connection of devices through communication networks."[16] Devices connected to the IoT have "a unique and assigned Internet identifier, through Bluetooth, or other communication protocol addresses."[17] The Internet of Things will continue to become even more connected because new connectivity technologies, such as 5G, will allow more devices to connect to the Internet with less latency and strain on the network.[18] The application of AI and IoT into tangible network of interconnected "smart devices" has revolutionized our society by saving time, money, and energy.[19] These benefits have generated significant demand with the global smart home device market expected to reach $176.10 billion in 2026.[20] Major tech companies including Amazon, Google, and Apple have developed AI-powered smart devices such as Amazon Alexa, Google Assistant, and Siri. AI-powered smart devices

---

https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9046438&fileOId=9053657 [https://perma.cc/JXZ4-3ZAQ].

13. *Id.*; *see The European Union Agency for Cybersecurity (ENISA), IOT and Smart Infrastructures*, https://www.enisa.europa.eu/topics/iot-andsmart-infrastructures/iot [https://perma.cc/JXZ4-3ZAQ] (defining IoT as "a cyberphysical ecosystem of interconnected sensors and actuators, which enable intelligent decision making").

14. Johansson, *supra* note 12.

15. *Id.*

16. Geraint Howells & Christian Twigg-Flesner, *Interconnectivity and Liability: AI and the Internet of Things*, *in* THE CAMBRIDGE HANDBOOK OF A.I.: GLOB. PERSPS. ON L. & ETHICS 179, 180 (Larry A. DiMatteo et al. eds., 2022).

17. CPSC, *Potential Harms*, *supra* note 1.

18. Bob O'Donnell, *IoT For 5G Could Be Next Opportunity*, FORBES (June 17, 2021, 9:00 AM), https://www.forbes.com/sites/bobodonnell/2021/06/17/iot-for-5g-could-be-next-opportunity/?sh=107f5d8758e6 [https://perma.cc/ALY8-32N4].

19. Zac Amos, *Artificial Intelligence is the Next Step for Smart Homes*, UNITE.AI (Apr. 12, 2022), https://www.unite.ai/artificial-intelligence-is-the-next-step-for-smart-homes/ [https://perma.cc/9SVG-ABZM].

20. Research and Markets, *Global Smart Home Devices Market Report 2022: 17.5% Annual Growth Driven by Key Players ABB, General Electric, Amazon, Google & Others,* GLOBENEWSWIRE.COM (Sept. 1, 2022, 5:13 AM), https://www.globenewswire.com/en/news-release/2022/09/01/2508256/28124/en/Global-Smart-Home-Devices-Market-Report-2022-17-5-Annual-Growth-Driven-by-Key-Players-ABB-General-Electric-Amazon-Google-Others.html [https://perma.cc/QY4T-7BNJ].

can collect data and predict user behavior, and even develop situational awareness.[21]

B. Current Climate of AI and IoT

AI and "IoT devices have potential for doing much good in the world," as they "can increase convenience, enhance the quality of life, and even improve our health."[22] Smart devices hold "plenty of potential for consumer harm," including both physical and nonphysical injuries.[23] However, due to the rapid evolution of AI and IoT, our current legal landscape is struggling to catch up with finding legal tools to address these potential harms.[24]

There are a myriad of physical injuries that could arise from AI-powered smart devices including cooking appliances activated through cell phone apps creating fire hazards or app-controlled furnaces overheating; smoke alarms that do not activate nor provide correct information; brake malfunctions on bikes or scooters causing riders to be thrown off their vehicles; and even baby monitors providing incorrect information to caregivers.[25] These AI technologies are expanding rapidly and are causing traditional legal tools and remedies to be left behind.[26] The "impression of humans handing over control to machines" has "fueled a fear of emerging liability gaps," which could leave victims uncompensated and could hide responsibility behind a "software code nobody feels responsible for."[27] The new field of "AI torts" will encompass physical and emotional injuries caused by not only robots and autonomous vehicles, but also injuries from software algorithms powered by AI components and inflicted on people who have relied on AI's assistance in all various tasks.[28]

Nonphysical harms from AI could include discrimination from algorithmic bias, reputational harm, or even data and privacy concerns. Smart devices powered with AI and IoT are "likely to open up unprecedented opportunities for businesses to collect and analyze consumer data and communicate directly with consumers."[29] Though the legal field surrounding AI is still

---

21. Amos, *supra* note 19.
22. Kate Tokeley, *The Power of the "Internet of Things" to Mislead and Manipulate Consumers: A Regulatory Challenge*, 2 NOTRE DAME J. EMERGING TECH. 111, 116 (2021).
23. *Id.* at 117.
24. *Id.*
25. CPSC, *Potential Harms*, *supra* note 1, at 15.
26. Kalra, *supra* note 4, at 9.
27. Christiane Wendehorst, *Strict Liability for AI and other Emerging Technologies*, 11(2) J. EUROPEAN TORT L. 150, 150 (2020).
28. Amy L. Stein, *Assuming the Risks of Artificial Intelligence*, 102 B.U. L. REV. 979, 982 (2022).
29. Tokeley, *supra* note 22, at 114.

developing, consumers "refuse to forego the usage of AI entities in commercial and noncommercial uses," and thus either purposefully or implicitly tend to recognize that the advantages of AI outweigh potential inherent flaws or unforeseen danger.[30]

So far, product liability law has been applied to a limited scope of AI-related products, such as autopilot in airplanes and vehicle features like cruise control and automatic parking.[31] When considering AI claims under product liability law, there is a "careful balancing of holding tortious actors liable and encouag[ing] technological innovation."[32] Liability rules are key to influencing companies' behavior and will influence how much AI companies decide to invest in developing safer technology.[33] If product liability law is used in AI lawsuits, it runs the risk of providing insufficient incentives for safety if the AI company could be able to reduce its liability by showing a plaintiff was comparatively negligent.[34] To alleviate this potential risk, certain courts have held that some AI products are "'unavoidably unsafe' under the Restatements," and therefore companies failed to adequately warn consumers of the danger of the AI product and could not argue comparative negligence.[35]

When considering what liability scheme to use for AI, it is crucial to consider the risks posed by AI. Risks from AI "may arise from the data used to train the AI system, the AI system itself, the use of the AI system, or interaction of people with the AI system."[36] An additional risk of AI is what will happen when the system encounters a new situation. For example, a Tesla using autopilot crashed into a tractor trailer in Ohio because it "failed to recognize the white truck against the bright sky."[37] This was a

30. Lior, *supra* note 7, at 5–6.

31. Frank Griffin, *Artificial Intelligence and Liability in Health Care*, 31 HEALTH MATRIX 65, 79 (2021).

32. Suzanne McNulty, *AI Update: Artificial Intelligence and Products Liability,* GLOBAL AEROSPACE (Jan. 18, 2022), https://www.global-aero.com/ai-update-artificial-intelligence-and-products-liability/ [https://perma.cc/KG3S-7LG3].

33. Matthew Wansley, *The End of Accidents*, 55 U.C. DAVIS L. REV. 269, 272 (2021).

34. *Id.*

35. Griffin, *supra* note 31, at 93.

36. NAT'L INST. STANDARDS & TECH., AI RISK MANAGEMENT FRAMEWORK: SECOND DRAFT 1 (2023) https://www.nist.gov/itl/ai-risk-management-framework [https://perma.cc/YF7F-SRE2].

37. Neal E. Boudette, *Tesla's Self-Driving System Cleared in Deadly Crash*, N.Y. TIMES (Jan. 19, 2017), https://www.nytimes.com/2017/01/19/business/tesla-model-s-autopilot-fatal-crash.html [https://perma.cc/84FE-8QNT].

scenario the AI system had never encountered before, and the system malfunctioned in a way researchers and programmers did not expect.[38]

C. Strict Liability Overview

Strict liability is a no-fault based liability regime and the current standard is set for all products, including AI, by the Product Liability Directive in the European Union.[39] Strict liability emerged in the industrial era "when the introduction of new machines and natural forces into common use increased the level of risk in social life."[40] Strict liability has been considered a cost allocation system intended to achieve numerous goals including "wealth redistribution, efficiency, [and] autonomy. . . ."[41] Applied to products, strict product liability is when a seller, distributor, or manufacturer of a product is liable for injuries caused by the defective product, regardless of whether the defendant was negligent.[42] Generally, for a plaintiff to establish a claim, the plaintiff must demonstrate three elements: (1) a defective product, (2) causation between the defective product and the plaintiff's injury, and (3) proof that the defect already existed when "the product left the manufacturer's control."[43] Under strict products liability, however, "[p]roducts manufacturers can be held responsible any time they release items to the public that directly cause harm, even if they didn't engage in any specific actions (or inactions) that led to the problems occurring."[44]

Though less is required to prove fault under strict liability than in other liability regimes, this does not mean liability is assigned automatically. Defendants may raise several defenses including assumption of the risk, misuse of the product, or the "state-of-the-art" defense to offset liability. Most applicable to AI is the state-of-the-art defense. This is a European defense which states that a Producer is not liable if "the state of scientific

---

38. *See id.*

39. Council Directive of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products 85/374/EEC, O.J. (L 210). 1. *See also Commission Proposal for a Directive of the European Parliament and of the Council on Liability for Defective Products,* at 3, COM (2022) final (Sept. 28, 2022) [hereinafter *Revised Products Liability Directive*] (The revised product liability directive applies the directive to defective AI systems that cause "physical harm, property damage, or property loss").

40. PAWEL KSIĘŻAK & SYLWIA WOJTCZAK, TOWARD A CONCEPTUAL NETWORK FOR THE PRIVATE LAW OF ARTIFICIAL INTELLIGENCE, 239, 280 (Casanovas et. Al. eds., 2023).

41. Martin A. Kotler, *Reconceptualizing Strict Liability in Tort: An Overview*, 50 VAND. L. REV. 555, 560 (1997).

42. Christy Bieber, *What is Strict Product Liability? Definition & Examples,* FORBES ADVISOR (Jan. 18, 2023), https://www.forbes.com/advisor/legal/product-liability/strict-product-liability/ [https://perma.cc/2MRG-VQAN].

43. Griffin, *supra* note 31, at 92.

44. Bieber, *supra* note 42.

and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered."[45]

III. RECENT REGULATORY AND LEGISLATIVE GUIDANCE

With AI technology evolving rapidly, governmental agencies have struggled to keep pace and enact legislation to address emerging liability concerns. However, in the past two years, many regulatory and governmental agencies have published reports and recommendations on how both the legislature, as well as companies and consumers, should think about AI.[46] When considering AI, different governments must decide how they would like to balance innovation versus safety. The more regulation passed, the more likely innovation will be stifled by increased business costs and risks.[47] However, a lack of appropriate regulation can make it very challenging for consumers to have legal remedies for harms suffered.[48] Governments have taken differing approaches to weighing this balance in recent years. The UK, for instance, "appears to be taking an approach that favors innovation over regulation."[49] However, the U.S., which has historically favored innovation over regulation may see increased "government scrutiny and regulation of AI tools" in 2023 and beyond.[50]

---

45. Tiago Sergio Cabral, *Liability and Artificial Intelligence in the EU: Assessing the Adequacy of the Current Product Liability Directive*, MAASTRICHT J. EUROPEAN COMPARATIVE L. 615, 618 (2020).

46. *See generally* CPSC, *Potential Harms*, *supra* note 1; *A European Approach to Artificial Intelligence*, EUR. COMM'N, https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence [https://perma.cc/MX72-6KRT] (last visited July 29, 2023); *Artificial Intelligence*, U.S. DEP'T OF STATE, https://www.state.gov/artificial-intelligence/ [https://perma.cc/UT9XEWNX].

47. *See* Jack Kelly, *Artificial Intelligence is Getting Regulated*, FORBES (June 5, 2023), https://www.forbes.com/sites/jackkelly/2023/06/05/artificial-intelligence-is-getting-regulated/?sh=21f48ac57a09 [https://perma.cc/6LBQ-WARX].

48. *See id.*

49. Alistair Maughan, *AI Trends for 2023 - UK Targets Innovation Not Regulation for AI Sector*, MORRISON FOERSTER: MOFO TECH (Jan. 17, 2023), https://mofotech.mofo.com/topics/ai-trends-for-2023-uk-targets-innovation-not-regulation-for-ai-sector [https://perma.cc/PT2A-N95W].

50. Tessa Schwartz & Heather M. Whitney, *AI Trends for 2023 - Increased Government Scrutiny of AI,* MORRISON FOERSTER: MOFO TECH (Dec. 21, 2022), https://mofotech.mofo.com/topics/ai-trends-for-2023-increased-government-scrutiny-of-ai [https://perma.cc/D6ZB-CSP9].

This section will examine both the EU's uniform AI regulation and multiple U.S. agency's recommendations on AI guidance as of spring 2023 to determine how future U.S. regulation may unfold.

A. EU Guidance on AI Regulation

The EU has emerged as a world leader in AI legislation and plans to invest one billion dollars annually in AI programs, with an eventual target investment volume of twenty billion pounds per year.[51] Currently, the EU has the most developed regulation concerning AI and serves as a model for what regulations other countries could potentially enact in the future.[52] One of the crucial pieces of regulation enacted by the AI that will serve as a roadmap for where U.S. regulation may go is the 2022 revision to the EU Product Liability Directive.

1. 2022 Draft Revision to the EU Product Liability Directive

On September 28, 2022, the EU Commission Published their draft revision to the EU Product Liability Directive (hereinafter "PLD") as an attempt to respond to many of the issues raised with the PLD's ability to govern AI and evolving technology.[53] The council explicitly states how these revisions were needed because the current "PLD's decades-old definitions and concepts," are unable to be applied to "products in the modern digital economy and circular economy (e.g., software and products that need software or digital services to function, such as smart devices)."[54] Further, the council notes the current burden of proof under the PLD is "challenging for injured persons in complex cases," especially in the case of smart products or AI-enabled products.[55]

The revision first clarifies definitions within the PLD and explains the directive's scope. The proposed revision "confirm[s] that AI systems and AI-enabled goods are 'products' and therefore fall within the PLD's scope, meaning that compensation is available when defective AI causes damage, without the injured person having to prove the manufacturer's fault."[56] The proposed revision goes on to explicitly state that "products in the digital

51. *A European Approach to Artificial Intelligence*, EUR. COMM'N, https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence https://perma.cc/MX72-6KRT].

52. *See* Kelvin Chan, *How Europe is Leading the World in the Push to Regulate AI*, ASSOCIATED PRESS (June 13, 2023), https://apnews.com/article/ai-act-artificial-intelligence-europe-regulation-94e2b38703b38fdbfabc9580f845ef9a [https://perma.cc/EM99-L9PW].

53. *Revised Products Liability Directive*, *supra* note 39, at § 1.1.

54. *Id.*

55. *Id.*

56. *Id.* at § 1.3.

age can be tangible or intangible," meaning that software "is capable of being placed on the market as a standalone product [or] may [] be integrated into other products as a component, and is capable of causing damage through its execution."[57]

The proposal also addresses a company's potential liability under the PLD.[58] First, the proposal confirms "that manufacturers can be held liable for changes they make to products they have already placed on the market, including when these changes are triggered by software updates or machine learning."[59] Second, the proposal expands potential liability by stating that "the developer or producer of software" will be treated as the manufacturer for liability purposes.[60] Finally, the proposal limits the amount of time available to bring a claim.[61] The council argues that based on the rapid advancement of technology and the natural increase in safety standards over time, manufacturers should not be liable for unlimited periods of time for defectiveness of their products.[62] Liability will be subject to a reasonable length of time of "10 years following placing on the market, without prejudice to claims pending in the legal proceedings," or 15 years where symptoms of personal injury are slow to emerge.[63]

The revision provides many insights into the council's commitment to fairly apportion risk between AI companies and their consumers.[64] In order to achieve a fair apportionment of risk based or no-fault liability, the revision places the burden of proof on the injured party to prove a causal link between the damage endured and the defective product.[65] However, the council proposed that "in order to reflect the increasing prevalence of inter-connected products, the assessment of a product's safety should also take into account the effects of other products on the product in question," and should further consider "the effect on a product's safety of its ability to learn after deployment."[66] The revision responds to calls of the European Parliament to ensure liability rules are adapted to AI by alleviating the "burden

57. *Id.* at 15.
58. *See id.* at § 1.3.
59. *Revised Products Liability Directive*, *supra* note 39, at § 1.3.
60. *Id.* at 16.
61. *See id.* at 22–23.
62. *Id.* at 22.
63. *Id.*
64. *See id.* at § 1.1.
65. *Id.* at 19.
66. *Revised Products Liability Directive, supra* note 39, at 17.

of proof in complex cases, which could include certain cases involving AI systems, and when products fail to comply with safety requirements."[67]

Finally, the revision maintains the state-of-the-art defense, which states that "manufacturers should also be exempted from liability if they prove that the state of scientific and technical knowledge" was cutting-edge at the time the AI was released.[68] This "state" is determined by the most advanced objective knowledge available while the product was within the manufacturer's control.[69] This is not determined by the manufacturer's actual knowledge.[70] Maintaining the state-of-the-art defense gives companies at the cutting-edge of AI technology a wide safety net to fall back on if litigation emerges.

The PLD revision places the EU at the forefront of AI regulation worldwide, and may serve as a preview for potential future regulations enacted in the U.S.

B. U.S. Guidance on AI Regulation

Current U.S. guidance on AI regulation can be confusing for both companies and consumers alike. Overlap in jurisdiction between different agencies, multiple models proposed to analyze AI and its harms, and the fact that nothing currently published is binding makes evaluating AI risks especially challenging. This section will examine reports from four U.S. agencies to provide a snapshot of U.S. guidance as of spring 2023 and lay a foundation for recommendations on future U.S. regulation.

The U.S. has a history of favoring innovation over regulation. The First Amendment to the United States Constitution, specifically, has protected technology from "interference and meddling form the regulatory state" which has given the U.S. a competitive advantage over other countries with stricter regulatory schemes.[71] Major competitors in the technology sector, including Google, Facebook, and Amazon tend to come from the U.S. rather than from European countries, largely due to this protection from regulation.[72]

In a 2018 Homeland Security report, the government recognized the importance of beginning a dialogue intended to develop frameworks for AI to "reduce the risk from use, misuse, and exploitation of AI, without

---

67. *Id.* at § 1.3.
68. *See id.* at 22.
69. *Id.* at 22.
70. *Id.*
71. James Pethokoukis, *Is Regulation Slowing Tech Progress and Innovation? A Long-read Q&A with Eli Dourado,* AEI.ORG (June 3, 2016), https://www.aei.org/economics/big-government-regulation-slowing-tech-progress-eli-dourado/ https://perma.cc/6VFZ-G3HL].
72. *Id.*

impeding the United States' technological development and competitive advantage."[73] This report explored the characteristics any future AI regulation should have, and emphasized the importance of flexibility to allow the framework to evolve with innovation and "create buy-in within all appropriate private and public sector entities."[74]

In 2024, the U.S. will likely see enhanced priorities to "measure and evaluate AI technologies through standards and benchmarks, [and] develop shared public datasets for environments for AI training and testing, and to ensure the safety and security of AI systems."[75] In the past three years, there have been dozens of white papers published surrounding potential AI regulations. A white paper is a broad policy document that provides commentary and potential guidelines, however, is not legally binding.[76] Many U.S. agencies, including the Federal Drug Association ("FDA"), Consumer Product Safety Commission ("CPSC"), Federal Trade Commission ("FTC"), and the Department of Homeland Security ("DHS") have released their recommendations and outlook on AI and smart devices within their respective agencies. However, all these recommendations are exactly that – merely recommendations. There has been no uniform national legislation or regulation on AI and smart devices.

The U.S. Department of State has recognized the importance of forming an international policy around AI and engage in "various bilateral and multilateral discussions to support responsible development, deployment, use, and governance of trustworthy AI technologies."[77] Several U.S. agencies increased AI funding in 2022, including the National Institute of Standards and Technology ("NIST") which plans to increase its AI research by $33.3 million, the Department of Defense ("DoD") which increased its AI budget

73. HOMELAND SEC., 2018 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM SYNOPSIS 2 (2018).

74. HOMELAND SEC., USING STANDARDS TO MITIGATE RISKS 3 (2018).

75. Erin M. Bosman & Matt Robinson, *AI Trends For 2023 - Budgeting For the Future of AI,* MORRISON FOERSTER: MOFO TECH (Dec. 29, 2022), https://mofotech.mofo.com/topics/ai-trends-for-2023-budgeting-for-the-future-of-ai [https://perma.cc/4XHN-DP94] (citing NETWORKING & INFO. TECH. RSCH. & DEV. PROGRAM & NAT'L A.I INITIATIVE OFF., SUPPLEMENT TO THE PRESIDENT'S FISCAL YEAR 2023 BUDGET (Dec. 2022) https://www.nitrd.gov/pubs/FY2023-NITRD-NAIIO-Supplement.pdf [https://perma.cc/M4KL-LYKG]).

76. Kenneth W. Gideon & William J. Wilkins, *The Evolution of Government Submissions*, 68 TAX L. 79, 80 (2014), https://www.jstor.org/stable/24247823 [https://perma.cc/LKQ9-DT83].

77. *Artificial Intelligence*, *supra* note 46.

by $38.2 million, and the Department of Energy ("DoE") which requested an additional $26.2 million for AI research.[78]

1. 2023 NIST AI Risk Management Framework

On January 26, 2023, the National Institute of Standards and Technology published their voluntary "Artificial Intelligence Risk Management Framework," a document designed to give companies aid in managing the risks of AI when creating and deploying trustworthy and responsible AI systems.[79] The NIST instructs companies when thinking about risks to consider the potential negative impact or levels of potential harm incurred if the event occurs and the likelihood that the harm actually takes place.[80] However, risk may present differently at different stages of the product life cycle. As the AI evolves, the nature and severity of associated risks may also evolve, making it crucial to measure risks throughout the entire life cycle of the AI.[81]

The NIST encourages companies to create both accountability mechanisms for AI as well as develop roles and incentives for risk management strategies to be effective.[82] In order to develop responsible AI, companies must have trust, transparency, reliability, and understanding.[83]

2. FDA AI Guidance

The FDA actively monitors the use of AI and machine learning software and has begun developing a proposed regulatory framework.[84] In April 2019, the FDA published their proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)—Based Software as a Medical Device (SaMD)—Discussion Paper and Request for Feedback.[85] Then, in 2021, the FDA published its AI and Machine

78. Bosman & Robinson, *supra* note 75.

79. NAT'L INST. STANDARDS & TECH., ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK (AI RMF 1.0) 1, 2 (2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf [https://perma.cc/S2CZ-YCZL].

80. *Id.* at 4.

81. *Id.* at 6.

82. *Id.* at 9.

83. *Id.* at 12–15.

84. FDA, PROPOSED REGULATORY FRAMEWORK FOR MODIFICATIONS TO ARTIFICIAL INTELLIGENCE/MACHINE LEARNING (AI/ML)-BASED SOFTWARE AS A MEDICAL DEVICE (SAMD)—DISCUSSION PAPER AND REQUEST FOR FEEDBACK (2019), https://www.fda.gov/files/medical%20devices/published/US-FDA-Artificial-Intelligence-and-Machine-Learning-Discussion-Paper.pdf.

85. *See* Nathan A. Brown et al., *FDA Releases Action Plan for Artificial Intelligence/ Machine Learning- Enabled Software as a Medical Device*, 4 J. ROBOTICS, A.I. & L. 255, 255–56 (2021).

Learning Action Plan, which laid out additional steps the FDA plans to take, such as "continuing to develop its own proposed regulatory framework for draft guidance on a predetermined change control plan for software learning," and "developing new methods to evaluate and improve ML algorithms."[86] "[T]he FDA [recommends] 'Good Machine Learning Practices' to describe [. . .] AI/ML best practices, including data management, feature extraction, training, interpretability, evaluation, and documentation."[87]

To ensure "the risk and impact of an unfair or negative outcome" of an AI product is not high, the FDA has only authorized the use of "locked algorithms," which are algorithms that "don't learn every time the product is used and therefore don't change[. . . .]"[88] This has allowed the FDA to evaluate algorithms with fixed outcomes (e.g., a specific input will always yield a specific output); however, as the use of ML algorithms becomes more widespread, pressure for methods to evaluate dynamic algorithms will only continue to grow.

3. 2022 CPSC Guidance on AI

The CPSC has been active in the discussions surrounding AI for consumer products. On March 31, 2022, CPSC staff held an "AI/ML Forum to garner stakeholder input on concerns and approaches to addressing this new technology."[89] This forum focused on the analysis of consumer products using AI/ML technologies to determine whether these products "pose an unreasonable risk of harm for consumers."[90] In response to this forum, the CPSC recommended voluntary standards for the development of consumer products which use AI and ML technologies.[91]

The CPSC recommends the following four-step approach to evaluating AI in consumer products: (1) "screen consumer products and identify the existence of AI/ML technologies," (2) "assess capabilities and determine

86. *Id.*
87. *Id.* at 258.
88. Francois Candelon et al., *AI Regulation Is Coming: How to Prepare for the Inevitable*, HARV. BUS. REV., (Sept.—Oct. 2021), https://hbr.org/2021/09/ai-regulation-is-coming [https://perma.cc/UWC2-L683].
89. CPSC, *Potential Harms*, *supra* note 1, at 20.
90. U.S. CONSUMER PROD. SAFETY COMM'N, APPLIED A.I. & MACHINE LEARNING TEST & EVALUATION FOR CONSUMER PRODS. 2 (Aug. 24, 2022), https://www.cpsc.gov/s3fs-public/Applied-Artificial-Intelligence-and-Machine-Learning-Test-and-Evaluation-Program-for-Consumer-Products.pdf [hereinafter CPSC, *Applied AI*].
91. CPSC, *Potential Harms*, *supra* note 1, at 20.

the implications of these technologies," (3) "analyze contributing factors that AI/ML have to discern if hazardous," and (4) "monitor/measure conditions to determine if/when AI/ML evolves beyond safe parameters."[92]

The CPSC believes the assessment of AI products should be done by subject matter experts who should "establish[] a test plan to characterize AI/ML "capabilities relative to their function within the system."[93] Assessing the AI relative to its role provides the subject matter experts the ability to effectively test AI technologies.[94] The AI/ML must also be considered to the extent it contributes to the product, and specifically whether it contributes to a safety hazard.[95] This analysis includes determining whether there are a variety of environmental conditions that could affect the product design in reasonably foreseeable ways.[96]

In its report, the CPSC addressed a key issue that is consistent among U.S. guidance: how the implementation of various voluntary guidelines and "best practices" will "require extensive collaboration," given each agencies' limited resources.[97] The CPSC proposes collaboration among various federal agencies and continued "contributions to public-private partnerships like ACT-IAC" to create unified voluntary standards and work towards a method of enforcement.[98]

4. 2022 FTC Report to Congress

On June 16, 2022, the Federal Trade Commission ("FTC") published a report to Congress that reviewed online harms from AI.[99] Key takeaways from the FTC's report are the importance of diversity when building and implementing AI, and transparency for consumers to know how the AI is working.[100]

The FTC argued that the scientists and companies building and employing AI tools are "responsible for both inputs and outputs."[101] Therefore, it is their responsibility to hire diverse teams to diminish "inadvertent bias or

92. CPSC, *Applied AI*, *supra* note 90.
93. *Id.* at 12.
94. *Id.*
95. *Id.*
96. *Id.* at 13.
97. *Id.* at 15.
98. CPSC, *Applied AI*, *supra* note 90, at 15.
99. FTC, REPORT TO CONGRESS: COMBATTING ONLINE HARMS THROUGH INNOVATION 1, 7 (June 16, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Combatting%20Online%20Harms%20Through%20Innovation%3B%20Federal%20Trade%20Commission%20Report%20to%20Congress.pdf [https://perma.cc/3HG3-GBZD] [hereinafter FTC Congress Report].
100. *Id.*
101. *Id.*

discrimination, and to avoid using training data and classifications that reflect existing societal and historical inequities."[102] To ensure there is no inadvertent bias or discrimination, there must be "[a]ppropriate documentation of the datasets, models, and work undertaken" to record the impact and actual outcomes.[103]

The FTC emphasized the need to protect against inadvertent bias in response to numerous AI deployed over the last few years that resulted in serious harms due to bias.[104] In 2017, Amazon was forced to discard an AI recruiting tool that discriminated against women.[105] The AI was designed to sort through resumes to identify talent.[106] However, the AI was trained by previous resumes submitted to the company over 10 years, and subsequently taught itself that male candidates were preferable to women because of the male dominance in past applications.[107] In 2018, a Michigan man was arrested after a biased AI matched his driver's license to a blurry photo of a suspect.[108] Both MIT and NIST have published studies which show that while facial recognition may work well on white men, it may falsely identify ten to one hundred times more African-American or Asian faces as opposed to Caucasian faces.[109] Recently in November 2022, after being made public for a mere three days, Meta was forced to take down their latest AI tool, Galactica, because it began to produce biased content.[110] Galactica was created to assist with scientific tasks and was intended to be able to create its own scientific papers and Wikipedia style pages.[111] The AI had to be taken down after it began to

102. *Id.*
103. *Id.*
104. *Id.*
105. Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women*, REUTERS (Oct. 10, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G [https://perma.cc/7GLY-VYEQ].
106. *Id.*
107. *Id.*
108. Kashmir Hill, *Wrongfully Accused by an Algorithm*, NY TIMES (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/V6U8-52RZ].
109. *Id.*
110. Leigh McGowran, *Meta's 'Biased' Science-Writing AI Demo Gets Pulled After Three Days*, SILICON REPUBLIC (Nov. 22, 2022), https://www.siliconrepublic.com/machines/galactica-meta-ai-large-language-model [https://perma.cc/46L6-MM3L].
111. *Id.*

create biased articles that looked realistic but in reality amounted to pseudo-science.[112]

Transparency in AI is meaningful when it involves the "disclosure of intelligible information sufficient to allow third parties to test for discriminatory and harmful outcomes," and therefore allows "consumers to 'vote with their feet.'"[113] Companies must take additional steps to ensure AI tools are "explainable and contestable[,]" or else the AI tools "are merely 'black boxes' not worthy of trust."[114] Transparency is crucial to AI because it is one of the only ways there will be "real accountability."[115] "Real accountability" is when "the same [companies] that benefit from the advantages and efficiencies of algorithms [. . .] bear the responsibility of (1) conducting regular audits and impact assessments and (2) facilitating appropriate redress for erroneous or unfair algorithmic decisions."[116] The FTC recommended that "[p]latforms should be more open to sharing information" on AI-based tools, so the public is aware of "how AI-based tools are [. . .] used to filter certain content."[117] However, there must be a balance between being transparent with the public on how AI is used, and giving researchers "adequate legal protection to do their important work."[118]

One tool that may be used to promote transparency is Algorithmic Impact Assessments ("AIAs"), which can be used to assess AI systems in both the public or private sector.[119] These AIAs evaluate the "AI's system's impact before, during, or after its use."[120] When publicly shared, AIAs provide companies with accountability and could provide regulators with needed "information for investigations into deceptive and unfair business practices."[121] While the "need for AIAs is recognized broadly [. . .] both here and abroad[,]" there have only been proposed AIA frameworks suggested, which have yet to be implemented or put into practice.[122] With the need for AIAs also comes the need for certified, independent, and protected auditors to ensure the AIAs are successful when conducted.[123] It would also be beneficial to "create common definitions and standard metrics so that the public and researchers could make cross-

112. *Id.*
113. FTC CONGRESS REPORT, *supra* note 99, at 50.
114. *Id.* at 51.
115. *See id.*
116. *Id.* at 50–51.
117. *Id.* at 7.
118. *Id.*
119. FTC CONGRESS REPORT, *supra* note 99, at 55.
120. *Id.*
121. *Id.*
122. *Id.*
123. *Id.* at 56.

platform comparisons."[124] AIAs also require protections to be in place to protect whistleblowers who may "seek to report on harm or unfairness" of AI tools within a company.[125]

Finally, the FTC argued that for true transparency in AI's decision-making is crucial to focus on the entire AI lifecycle, from the design of the AI to its implementation.[126] The "designers and users of AI tools must nonetheless continue to monitor the impact of their AI tools, since fair design does not guarantee fair outcomes."[127]

5. U.S. AI Guidance Takeaways

In conclusion, U.S. AI guidance points to overarching themes of the need for accountability, transparency, diversity, and interpretability of AI. Additionally, there is a significant need for collaboration among governmental agencies in order to create unified AI standards. Current guidance reveals both the overlaps and gaps that have emerged in AI regulation due to the lack of uniform national standards.

IV. BENEFITS AND DRAWBACKS OF CURRENT LEGISLATIVE GUIDANCE ON AI

Current EU guidance suggests a strict liability scheme for consumer products with AI/ML. While the U.S. does not have an established liability scheme for addressing AI, it also appears to favor a strict liability regime.

A. Benefits of a Strict Liability Regime for AI

Strict liability is made problematic when applied to AI in the defect and causality requirements, where "AI's adaptive qualities and evolving independent decision-making capabilities" may cause challenges in "proving that damage caused by AI was due to a defect that was present when it left the producer's hands."[128]

Proponents of strict liability argue that by preventing complex and lengthy litigation, strict liability saves transaction costs "and places the blame on

124. *Id.* at 52.
125. FTC CONGRESS REPORT, *supra* note 99, at 56.
126. *Id.* at 58.
127. *Id.*
128. McNulty, *supra* note 32.

the actor in the best position to absorb or transfer the costs[.]"[129] Strict liability further reduces administrative costs by avoiding "the rigorous and problematic analysis of the 'reasonable person' standard."[130] Strict liability could be expanded to AI as it may be best suited to deal with the issues of autonomy and opacity of AI.[131] Further, proponents of strict liability argue that because "AI algorithms are 'black boxes,' the concept of algorithmic negligence is far too complex and opaque to be analyzed and evaluated by judges and juries."[132]

In conclusion, implementation of a strict liability regime would offset AI's inherently dangerous risks, and also allow AI tort law to be built upon a foundation of reciprocal risk analysis in which both companies and consumers are incentivized to reduce harmful AI activity. Because AI engages in "high levels of repetitive, ubiquitous activity," it creates "nonreciprocal risks, even if all parties take reasonable precautions."[133] A strict liability regime would balance these risks by giving companies an incentive to reduce harmful levels of activity because the companies would know they would be liable for any damages that may occur.[134] As a result, strict liability may further provide an incentive for companies to develop inherently safer technologies from design to implementation rather than simply minimizing harmful activity.[135] It could be argued that the nonreciprocal risks associated with AI make a strict liability regime more efficient than a negligence model to deal with AI harms.[136]

Generally strict liability also generates less reputational effects than a negligence model.[137] Typically, "economic analysis views strict liability as preferable to negligence because it is easier to administer and leads to better risk reduction."[138]

Considering potential challenges for consumers to prove fault, some have argued for the imposition of strict liability for AI cases. However, many

---

129. Anat Lior, *AI Strict Liability Vis-A-Vis AI Monopolization*, 22 COLUM. SCI. & TECH. L. REV. 90, 94 (2020).

130. *Id*. at 96.

131. *See* Wendehorst, *supra* note 27, at 159.

132. Lior, *supra* note 129.

133. *Id.* at 96.

134. *Id.*

135. *See* Wansley, *supra* note 33, at 330 ("A strict liability or no-fault system would create some incentive for AV companies to further develop AV technology's crash prevention potential.").

136. Lior, *supra* note 7, at 1119.

137. Assaf Jacob & Roy Shapira, *An Information-Production Theory of Liability Rules*, 89 U. CHI. L. REV. 1113, 1115 (2022).

138. *Id.* at 1113.

are concerned using strict liability for AI cases could have a "chilling effect. . . on the advancement of technology" and innovation.[139]

B. Problems with a Strict Liability Regime for AI

While using strict liability to address AI harms would provide many benefits, it would also raise policy issues, consumer suit issues, specific challenges due to the nature of IoT, challenges in proving responsibility, and significant affirmative defenses.

1. Policy Challenges with Strict Liability for AI

Numerous policy issues arise when considering a strict liability model. These issues are mostly centered around the detriment to innovation and effects strict liability could have on small businesses. A strict liability model normally carries greater costs to companies than a negligence regime, and thus could lead to smaller companies falling into bankruptcy or choosing to close and remove themselves from the market to avoid bankruptcy.[140] The second large policy problem for strict liability is the hurdle it could pose to innovation. Strict liability would enact a larger barrier for entrepreneurs to enter commercial markets and could prevent the development of new technologies and services.[141] Further, some have argued that it is inherently "unfair to impose strict liability for damage caused by devices that, by definition, can never be in full human-control."[142] While a negligence regime has the ability to accelerate market growth, because strict liability may stem innovation, it may also stem the market.[143]

A strict liability regime would also affect how companies are viewed in the consumer's eyes. Strict liability only shows that a specific harm occurred as a result of the defendant's activity.[144] A negligence model, on the other hand, is broader and "revolves around questions such as whether the harm was avoidable" or how the defendant compares to their industry competitors.[145] A negligence regime also "allows outside observers to

139. McNulty, *supra* note 32.
140. Lior, *supra* note 129, at 97.
141. *Id.* at 102.
142. Gupta, *supra* note 6, at 6079.
143. Cristina Carmody Tilley, *Just Strict Liability*, 43 CARDOZO L. REV. 2317, 2333 (2022).
144. Jacob & Shapira, *supra* note 137, at 1113.
145. *Id.* at 1115.

infer whether the past accident is indicative of the defendant's future behavior or not, which in turn affects their willingness to do business" with that company moving forward.[146] While a strict liability model may be easier to apply and easier for plaintiffs to sue under, a negligence model may allow consumers to make a more informed choice when evaluating AI products.

A final policy issue arises when looking at the scope of the risks presented by AI. If, for instance, a medical robot is more accurate and precise than a surgeon, and the patient would prefer to be operated on by the robot, "why should the hospital be punished with the more severe regime of liability (strict liability) for using the robot than a human surgeon (fault liability)?"[147]

2. Consumer Suit Challenges Related to Strict Liability

Another issue posed by strict liability is the ability for consumers to prove causation in product liability suits. AI presents many challenges for causation, including the following scenarios: (1) the AI could have worked as the manufacturer intended, however, the AI's self-learning abilities caused the malfunction;[148] (2) AI embedded in hardware may cause harm due to flaws of the hardware itself, due to its AI features, or because the latter caused the former to fail;[149] (3) the AI could be influenced by human conduct which creates difficulties when identifying the cause of the harm;[150] and (4) many smart devices have multiple AI systems which interact with each other, adding additional difficulty to identifying the principle cause of the harm.[151]

Consumers will further face difficulties in proving causation because "most claimants do not have the relevant information and/or technical expertise to demonstrate a causal link between the defendant's wrongdoing and the harm suffered."[152] Even in cases where a "claimant had relevant information, it would be very difficult, time-consuming and expensive to analyze the data to provide evidence of how the damage was caused."[153]

---

146. *Id.* at 1113.
147. KSIĘŻAK & WOJTCZAK, *supra* note 40, at 281.
148. *See* Emiliano Marchisio, *In Support of "No-fault" Civil Liability Rules for Artificial Intelligence*, 54 SN SOC. SCI.,1, 19 (2021).
149. *See id.* at 4.
150. *See id.* at 9.
151. *See id.* at 6.
152. Sadie Whittam, *Mind the Compensation Gap: Towards a New European Regime Addressing Civil Liability in the Age of AI*, 20 INT'L J.L. INFO. TECH. 249, 251 (Sept. 8, 2022).
153. *Id.* at 241–52.

A strict liability model runs the risk of leaving injured consumers without redress due to the challenges posed in bringing a valid suit.

3. Specific IoT Challenges with Strict Liability

Many problems arise when attempting to apply strict liability to IoT. The biggest drawback is the challenge in determining fault. If all products are connected, questions arise of how much a connected network of smart devices working in tandem share liability. In a world where smart devices make decisions based on data and a network of other smart devices, what happens when a device owned by one company makes a decision based off influence from a smart device owned by a separate company? What happens if these companies are using separate AI algorithms and are learning and acting in contrary ways? Although it "is usually very simple to say which component ultimately caused the damage in a more physical sense," it may become nearly impossible "to identify which component of a complex and connected digital ecosystem has caused the harm by being defective."[154]

Further issues arise in the context of "black-box AI." Black-box AI models are "created directly from data by an algorithm, meaning that humans, even those who design them, cannot understand how variables are being combined to make predictions."[155] Because of the disconnect between the models and humans, "it is not always possible for the developer to understand an AI's decision after it employed its self-learning capabilities."[156] If the developer is not even able to understand why an AI made a decision, it will be even more challenging for courts to "link a defective AI-enabled decision with damages occurred."[157]

4. Challenges of Accountability Under Strict Liability for AI[158]

The largest issue with a strict liability regime for AI is the question of accountability. Under strict liability, numerous companies could potentially be held responsible, including the producer, the frontend operator, and/or

154. Wendehorst, *supra* note 27, at 160.
155. Cynthia Rudin & Joanna Radin, *Why Are We Using Black Box Models in AI When We Don't Need To? A Lesson from an Explainable AI Competition*, 1(2) HARV. DATA SCI. REV. 1, 3 (2019).
156. Cabral, *supra* note 45, at 625.
157. *Id.*
158. Wendehorst, *supra* note 27, at 156.

the backend operator. The EU finds that the liable party is "the party that has to make sure the technology is safe when put into circulation and remains safe throughout its life-cycle."[159] The EU gives the producer the responsibility to take appropriate action if the technology ever becomes unsafe.[160] This seems like a sensible approach as generally the producer has the "highest degree of control concerning the interaction of the product with other components of digital ecosystems."[161]

However, there are many different parties that may be considered a "producer," thus, many parties may be held accountable. A producer could be: "(i) the manufacturer of a finished product; (ii) the manufacturer of any component part; (iii) the producer of any raw material and; (iv) any person who presents himself as the product's producer."[162]

The EU attempts to solve problems of accountability by allowing an injured party to seek damages against any potentially accountable parties.[163] In the EU, "when no Producer can be identified, every supplier in the supply chain can be called upon to answer as a Producer, unless the supplier is able to inform the injured party 'within a reasonable time, of the identity of the producer or of the person who supplied him with the product."[164]

It is not just the producer, however, who may be found accountable. Others have argued that is the frontend or backend operator who is more appropriate to bear responsibility for AI harms. The frontend operator is considered the owner or other long-term deployer of a device.[165] Some argue that when "considering the desire to achieve coherence with existing strict liability regimes under national law," it makes sense that "the party that decides about the concrete use of the device, bears both the economic risk of its operation and derives the economic benefits."[166]

The backend operator is defined as "any natural or legal person who, on a continuous basis, defines the features of the technology and provides data and an essential backend support service."[167] A backend operator thus "exercises a degree of control over the risk connected with the operation and functioning of the AI-system" and may be better suited to bear responsibility.[168]

---

159. *Id.* at 174.
160. *Id.*
161. *Id.*
162. Cabral, *supra* note 45, at 617.
163. *Id.*
164. *Id.*
165. Wendehorst, *supra* note 27, at 174.
166. *Id.* at 174–75.
167. *Id.* at 176.
168. *Id.*

Multiple theories of accountability and different approaches as to who should be held accountable can make strict liability difficult to adequately address AI harms.

5. Affirmative Defenses to AI Harms

An additional drawback to the EU's current liability scheme for AI is the state-of-the-art defense. This defense is a safeguard for companies and provides a very large blanket to shield large corporations from liability. The state-of-the-art defense states that a Producer is not liable if "the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered."[169] This defense risks perpetuating "inadequate and antiquated industry standards since future manufacturers will readily adopt the established industry standards" and receive a shield from strict liability through the state-of-the-art defense.[170] This has far-reaching implications for smart devices and for AI development in general. This defense has been characterized as a "Get Out of Jail Free" card for any company who can show that their AI had the most current algorithm at the time it entered the market, and thus use the defense as a shield against any lawsuits that may arise due to a malfunction or mis-action by the AI.

The court in *Commission v. United Kingdom* narrowed the uses of the state-of-the-art defense in the EU.[171] The court ruled that merely complying with industry standards and practices alone does not trigger this defense.[172] Rather, in order to evoke the state-of-the-art defense, a Producer "must prove compliance with the most advanced level of technical and scientific knowledge available at the time when the product was put into circulation even if it was not an industry standard."[173] Further, the knowledge in question is not "the state of knowledge of which the producer in question actually or subjectively was or could have been apprised, but the objective state of scientific and technical knowledge of which the producer is presumed to have been informed."[174] However, there is an exception to

169. Cabral, *supra* note 45, at 618.
170. Mark DeSimone, *The State-of-the-Art Defense in Products Liability: Unreasonably Dangerous to the Injured Consumer*, 18 DUQ. L. REV. 915, 921 (1980).
171. Cabral, *supra* note 45, at 622.
172. *Id.*
173. *Id.*
174. *Id.*

this general rule–the knowledge in question must have been available at the time.[175]

The Advocate General explains the question of knowledge accessibility by comparing "the scale of its dissemination between a study of a researcher in the United States published in an international English-language journal and similar research carried out by an academic in Manchuria published in the local scientific journal in Chinese" and not disseminated outside the region, and "states that it would be unrealistic for the producer to be aware of the latter."[176]

Though this case narrows the scope of the state-of-the-art defense, it still fails to protect consumers in the case that AI causes harm despite being the most advanced level of scientific and technical knowledge at the time it was released. The current revised draft of the PLD maintains the state-of-the-art defense, which will likely present significant challenges to consumers bringing suit, as companies will have an easy defense to argue.

V. SOLUTIONS AND PROPOSED LEGAL SCHEMES FOR AI

The drawbacks to a strict liability regime outweigh its benefits. Therefore, it is crucial to develop a different approach to regulate harms caused by AI. A multi-tiered liability scheme coupled with a voluntary ethical framework and regulatory agency dedicated solely to AI, would provide the flexibility required to deal with various types of AI harms. This proposed model would provide consumers with a way to be compensated for harms, while also protecting companies' innovative ability.

A. Multi-Tiered Liability for AI Regulation

A potential way to protect both consumers and companies would be a modified form of strict liability. As the foregoing analysis indicates, strict liability is not appropriate when pure economic or social risks are concerned, "unless further conditions are added, such as non-compliance with mandatory legal standards or some defect or malperformance," creating a variation of strict liability.[177] Other variations that could be beneficial to a modified form of strict liability include reversing the burden of proof. This could include "requiring the manufacturer or supplier to prove that the AI was not the cause of the harm;"[178] creating joint and several liability between

175. *Id.*
176. *Id.*
177. Wendehorst, *supra* note 27, at 159.
178. Phillip Kelly et al., *Man vs Machine: Legal Liability in Artificial Intelligence Contracts and the Challenges that Can Arise,* DLA PIPER LLP (Oct. 7, 2021), https://www.dlapiper.

"manufacturers, developers, suppliers and retailers;"[179] or adopting an adapted duty of care such as "obligations on a supplier of AI systems to monitor and maintain those systems to control for unexpected outcomes due to machine learning."[180]

However, the most effective way to address AI harms is to create a multi-tiered liability scheme that distinguishes between different types of harms and assigns different models of liability based on the type of AI that caused the harm.

The EU recently proposed the AI Act, which, if approved, would be the "first law on AI by a major regulator anywhere."[181] This proposed act could one day become the global standard for AI regulation.[182] This act would assign AI to one of three risk categories: (1) applications with unacceptable risk, "such as government-run social scoring of the type used in China, are banned," (2) applications that are high-risk, like a resume scanning tool to rank job applicants, would need to meet certain legal requirements, and (3) "applications not explicitly banned or listed as high-risk" would be largely left unregulated."[183] The EU defines their "risk" categories as the "social" risk the AI poses and therefore the harm it could do.[184] This proposed EU model could be used as a baseline to build a nuanced framework for regulating AI.

From a practical stance, it is also crucial to consider the risks of enforceability of different frameworks. One of the biggest drawbacks to a negligence model for AI regulation is the issues that arise with accountability and

---

com/en/romania/insights/publications/2021/10/man-vs-machine-legal-liability-artificial-intelligence-contracts/ [https://perma.cc/EZ72-S2JP].

179. *Id.*

180. *Id.*

181. *The Artificial Intelligence Act*, THE AI ACT, https://artificialintelligenceact.eu [https://perma.cc/39GD-4HE4]; *see Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206 final (Apr. 21, 2021).

182. *The Artificial Intelligence Act*, *supra* note 181; *see* Cecilia Kang & Adam Satariano, *As A.I. Booms, Lawmakers Struggle to Understand the Technology,* N.Y. TIMES (Mar. 3, 2023), https://www.nytimes.com/2023/03/03/technology/artificial-intelligence-regulation-congress.html [https://perma.cc/7L9A-6TEK] (Virginia Representative Donald S. Beyer, Jr. stated that "U.S. lawmakers would examine the European bill for ideas on regulation").

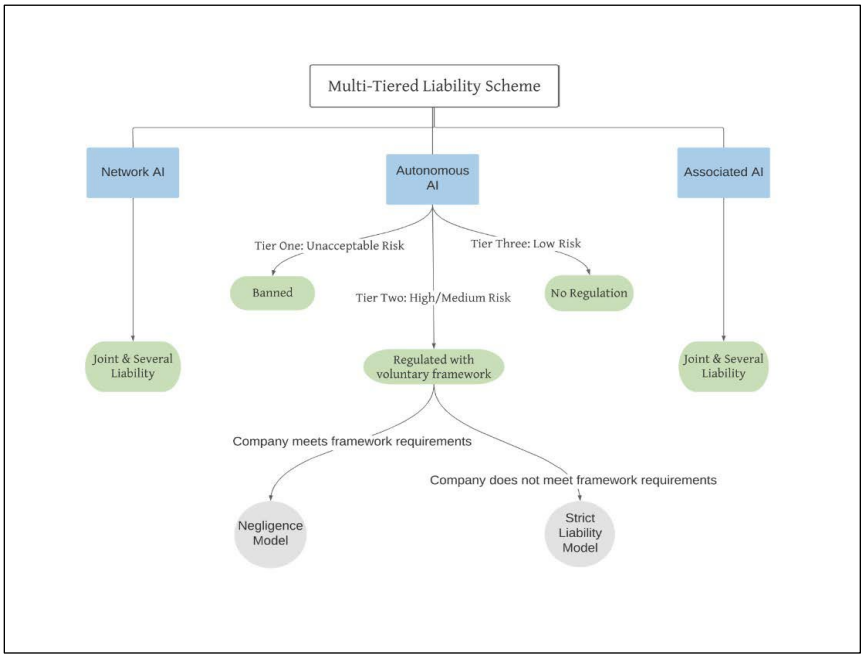
183. *The Artificial Intelligence Act*, *supra* note 181.

184. *Id.*

proving fault.[185] There must be tiers of regulation that not only reflect potential social risk as seen in the AI Act, but also reflect accountability. One way to accomplish this is to break down AI regulation into three different categories based on the three different types of accountability risks: (1) the autonomy risk, (2) the association risk, and (3) the network risk.[186]

1. Proposed AI Liability Scheme

AI liability should be structured commensurate with the three different types of AI risks, resulting in different regulations for network AI, autonomous AI, and associated AI. Both network and associated AI could be viewed through the lens of joint and several liability, and autonomous AI would be structured into three different tiers as seen below:



185. Andrew D. Selbst, *Negligence and AI's Human Users,* 100 B.U. L. REV. 1315, 1322 (2020) ("any attempt to solve AI problems with individual fault rules may be difficult.").

186. Klaus Heine & Alberto Quintavalla, *Bridging the Accountability Gap of Artificial Intelligence – What Can Be Learned from Roman Law?* LEGAL STUDIES 1, 4 (2023).

The most complicated category is autonomous AI. Autonomous AI is AI capable of making independent decisions based on data received.[187] The notion of electronic personhood has been raised to attempt to alleviate this risk.[188] Electronic personhood holds that sophisticated AI and "software agents may themselves be the addresses of legal duties and obligations as well as the holders of legal rights."[189] This has been a popular conversation in Europe after the European Parliament adopted a Resolution on Civil Law Rules on Robotics in 2017, which recommended that eventually "legislators should award legal personality to some very advanced AI systems."[190] AI's self-learning capabilities have been used by many to argue that AI may demonstrate a rationality through making independent decisions and therefore "should be held liable if it falls short of the parties' reasonable expectations in conducting that process."[191]

However, despite the initial attraction to electronic personhood, this concept fails due to its practical shortcomings. First, AI personhood does not make sense unless the AI has the financial means to pay compensation. For this concept to work, the AI must have a form of insurance to be able to pay for potential damages.[192] Further, most countries do not have a manner of implementing a new legal status attributed to AI.[193]

A more effective method to deal with the autonomy risk is a three-tiered system based in part on the EU AI Act. Tier One would encompass any AI deemed to be an unacceptable risk. This AI would be banned outright.[194] Tier Two would be any AI deemed to be either a medium or high risk. Tier Two would be regulated with a voluntary framework leading to two possible liability schemes. If a company meets the framework requirements, they would only be open to suits under a negligence model. On the other hand, if a company chooses not to comply with the voluntary framework, they would be subject to strict liability. The final Tier Three would be AI deemed to be low risk. This AI would not be subject to regulation and all liability would fall under a negligence scheme.

187. *Id.*
188. Wendehorst, *supra* note 27, at 155.
189. *Id.*
190. *Id.*
191. Kelly et. al., *supra* note 178.
192. Wendehorst, *supra* note 27, at 156.
193. Cabral, *supra* note 45, at 632.
194. If this AI is made, it would be subject to strict liability.

The second category of regulation would cover associated AI. The association risk of AI involves risks when AI and humans work together.[195] For instance, when a surgeon uses an AI hand to assist with a surgery. One solution to this risk is using contractual and non-contractual liability to ensure the human maintains their ethical obligations while recognizing that the decisions were made with the assistance of a machine.[196] The association risk may present challenges to consumers bringing suit by giving companies a means of arguing for the superseding cause doctrine.[197] For instance, when a Tesla autopiloted car crashed in 2016, Tesla tried "to shield itself from liability by pointing out that the negligent interactions of the driver were a more immediate cause of the crash, than the actions of the programmer."[198]

The most effective way to deal with the association risk would be under the multi-tiered liability scheme. This would hold associated AI liable under a joint and several liability standard. Under joint and several liability, multiple parties may be independently liable for the entire amount of injuries arising out of a tortious act. This would prevent companies from shifting the entirety of the blame to the human who made the decision along with the AI. For any autonomous associated AI, there would then be an analysis under the three-tier approach for autonomous AI. This analysis would determine whether negligence or strict liability would be imposed for the joint and several liability.

The final category of AI is network AI. The network risk describes the risk posed by IoT– namely when multiple AIs in a network learn from one another and coordinate their decisions.[199] When it comes to Blackbox AI within a network of AI controlled by various companies, responsibility can be near impossible to determine. A joint and several liability scheme could also be effective because it would allow the injured party to sue any of the companies who had an AI in the network but would also provide companies a defense if they can show that it was not their AI who was at fault. For any autonomous network AI, there would then be an analysis under the three risk tier approaches found under AI.

For any autonomous network AI, there would then be an analysis under the three-tier approach for autonomous AI. This analysis would determine whether negligence or strict liability would be imposed.

---

195. Heine & Quintavalla, *supra* note 186, at 5.
196. *Id.* at 6.
197. Weston Kower, *The Foreseeability of Human-Artificial Intelligence Interactions*, 96 TX. L. REV. 181, 184 (2017)
198. *Id.*
199. Heine & Quintavalla, *supra* note 186, at 7.

B. Proposed Uniform AI Ethical Framework

Critical to both the multi-tiered liability scheme and specifically the category of autonomous AI is the implementation of a voluntary ethical framework. Countless U.S. agencies have proposed various "ethical frameworks" or guidance for companies when dealing with AI. However, these agencies did not create these frameworks in collaboration with one another, so there is no uniformity among recommendations, and none of these rules are binding.

What would effectively help deal with AI liability is the enforcement of an "AI Ethical Guideline," which governs what companies are required to do to ensure their AI is ethical. This could then serve as a baseline for addressing liability when the AI harm in question is one of an ethical nature. This framework would incentivize companies to ensure their AI is complying with all ethical standards because it would allow consumers to choose which companies they wanted to use based on which were complying with the voluntary framework and would allow companies to be sued for liability under a negligence model rather than strict liability.

The American Council for Technology and Industry Advisory Council ACT-IAC proposed the Ethical Application of AI Index ("EAAI") framework, which is a starting point for building a uniform, enforceable ethical framework for AI. One important aspect of this framework is that it looks at the AI systems throughout the entire AI lifecycle, instead of concluding the framework once the AI is on the market.[200] Companies must ensure the AI is meeting the ethical framework throughout the entire life cycle of the AI, not just during its development.

Any uniform ethical framework must also include guidelines for diversity protections, transparency requirements, and continuous monitoring requirements. The possibility of discrimination within an AI system is rampant unless developers take active steps to ensure any possible bias is eliminated. An AI algorithm will reflect the "organization(s) and person(s) who implement and integrate the AI," and will equally reflect any implicit or explicit bias from those people and organizations.[201] Any uniform, ethical framework must require AI systems to be developed with diversity

200. ACT-IAC, ETHICAL APPLICATION OF ARTIFICIAL INTELLIGENCE FRAMEWORK: ACT-IAC WHITE PAPER 1 (Oct. 8, 2020), https://www.actiac.org/system/files/Ethical%20Application%20of%20AI%20Framework_0.pdf [https://perma.cc/J7V6-ZCDC].

201. *Id.*

"among various aspects including the team,"[202] and "with consultation from diverse communities, stakeholders, and domain experts."[203]

Companies and developers must also take a close look at the data to ensure there is no bias or discrimination. There must be protections against data bias within the AI, meaning that "AI systems should identify and address bias in the data to prevent negatively impacting individuals in promoted classes or status."[204] Along with protecting from data bias, there must be actions within the data modeling. AI algorithms work through learning from large quantities of data, so there must be actions and solutions to address any "biases inherently present in the data."[205] Unconscious bias is the result of "ingrained stereotypes, omission resulting from lack of awareness as to the variable's relevance . . . or even confirmation bias of data that results from prior association of the data with similar models."[206] Before an AI consumer product is brought to market, there should be pre-deployment testing to ensure the AI is safe, effective, and is not inadvertently discriminatory against a group of people.[207]

It is also important that the uniform ethical guideline accounts for some form of transparency within the AI system to ensure someone is accountable if harm occurs. This piece will be crucial to addressing future liability–if a company fails to meet the "transparency" requirement, this would be a clear indicator that strict liability rather than negligence should apply.[208] Transparency in AI should ensure that the AI "is explainable to any user, decision maker, or impacted population" to ensure AI data "is fair, interpretable, and representative."[209] Within an ethical framework, companies may have to be transparent about the purpose of the AI, the structure of the AI, and the "underlying actions of the algorithms used."[210] To qualify as "transparent," an AI must have "results from an algorithm [that] can be tracked back from a data, architecture and algorithmic perspectives."[211] It will be mandatory for companies to be transparent throughout the entire life cycle

202. *Id.* at 8.
203. WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY, BLUEPRINT FOR AN AI BILL OF RIGHTS: WHITE PAPER 5 (Oct. 3, 2022) [hereinafter WHITE HOUSE BLUEPRINT], https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf [https://perma.cc/NU6D-B545].
204. ACT-IAC, *supra* note 200, at 8.
205. *Id.* at 9.
206. *Id.* at 7.
207. WHITE HOUSE BLUEPRINT, *supra* note 203, at 15, 22.
208. *See* Wendehorst, *supra* note 27, at 159.
209. ACT-IAC, *supra* note 200, at 18.
210. *Id.*
211. *Id.*

of the AI, and companies may have to meet requirements of notifying consumers if the AI is significantly changed or updated.[212]

A transparency requirement may be challenging for companies to meet due to the popularity of "black box AI" and the difficulty involved in distinguishing how an AI made a decision. Due to the difficulty in meeting this requirement, regulators must give companies an incentive to do so. By allowing AI harms to fall under a negligence standard, if companies have complied with "Ethical Requirements," it would give companies sufficient incentive to work towards developing fair and transparent AI.

Finally, companies would have to meet ongoing monitoring requirements to comply with any uniform ethical framework. These procedures may include recalibration procedures, evaluation of performance metrics and harm assessments, and retraining of ML models as necessary to ensure that the AI's performance does not fall below an expected level and does not negatively evolve due to real-world or unexpected conditions.[213] As part of ongoing monitoring, it may be useful to require independent and ongoing evaluations conducted by ethics review boards or third-party auditors.[214] This monitoring should be conducted on a regular schedule or whenever a pattern of unusual results starts to occur.[215]

The EU has seen something acute to this concept in the form of non-compliance liability. Article 82 of the GDPR reflects this non-compliance liability, "which attaches liability to any infringement of the requirements set out by the GDPR."[216] There are specific liability regimes that attach liability to non-compliance with various standards,[217] and these regimes could be applied in the U.S. in the form of strict liability for non-compliance and negligence if companies comply with relevant standards.

C. Proposed AI Regulation Agency

U.S. regulatory agencies "arise to address new or newly acute challenges posed by big events or changes in behavior."[218] Historically, as new technologies have emerged, the U.S. has responded by creating regulatory

212. WHITE HOUSE BLUEPRINT, *supra* note 203, at 6.
213. *Id.* at 19.
214. *Id,* at 20.
215. *Id.* at 27.
216. Wendehorst, *supra* note 27, at 157.
217. *Id.*
218. Ryan Calo, *The Case for a Federal Robotics Commission*, BROOKINGS 1, 3 (Sept. 2014).

agencies designed to "oversee and investigate new technologies."[219] Just as the Nuclear Regulatory Commission ("NRC") was needed to investigate and regulate nuclear technology at the emergence of the nuclear age, a regulatory agency dedicated solely to artificial intelligence is needed today.[220] Currently, the U.S. government is operating through piecemeal: "agencies, states, courts, and others are not in conversation with one another,"[221] and instead each are all interpreting AI harms and how to address them independently.

Multiple different agencies have begun using existing laws in an attempt to regulate AI harms.[222] The FTC has entered into settlements with companies over AI facial recognition software in violation of FTC's consumer protection rules[223] and the Consumer Financial Protection Bureau ("CFPB") has cautioned companies that black-box AI systems could violate anti-discrimination laws.[224] Multiple agencies all attempting to regulate the field of AI will create both over- and under-regulation problems. Companies, consumers, and regulatory agencies will be left with uncertainty as to which agency will handle overlapping issues which will lead to inconsistent determinations and results. On the flip side, there may be other AI harms that don't appear to fall under any specific agencies purview and therefore run the risk of slipping through the cracks. The way to guard against over regulation while protecting consumers is by having a defined agency that would handle all AI regulation.

This AI regulatory agency would need to be responsible for three critical tasks: (1) deciding what AI systems are classified as–either unacceptable, high, medium, or low risk; (2) creating and maintaining an AI Ethical Framework for companies to follow, and (3) investigating and determining whether companies adequately followed the AI Framework when litigation arises.

---

219. Anton Korinek, *Why We Need a New Agency to Regulate Advanced Artificial Intelligence: Lessons on AI Congrol From the Facebook Files,* BROOKINGS.EDU (Dec. 8, 2021), https://www.brookings.edu/research/why-we-need-a-new-agency-to-regulate-advanced-artificial-intelligence-lessons-on-ai-control-from-the-facebook-files/ [https://perma.cc/77SS-N43B].

220. *Id.*

221. Calo, *supra* note 218, at 4.

222. Kang & Satariano, *supra* note 182.

223. *California Company Settles FTC Allegations It Deceived Consumers About Use of Facial Recognition in Photo Storage App*, FED. TRADE COMM'N (Jan. 11, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/01/california-company-settles-ftc-allegations-it-deceived-consumers-about-use-facial-recognition-photo [https://perma.cc/3XRM-Z8FE].

224. *CFPB Acts to Protect the Public from Black-Box Credit Models Using Complex Algorithms*, CONSUMER FIN. PROT. BUREAU (May 26, 2022), https://www.consumerfinance.gov/about-us/newsroom/cfpb-acts-to-protect-the-public-from-black-box-credit-models-using-complex-algorithms/ [https://perma.cc/WH4U-BK56].

Further responsibilities of an AI regulatory body may include powers to perform audits and impact assessments of advanced AI systems.[225]

VI. NEXT STEPS FOR U.S. COMPANIES, CONSUMERS, AND REGULATORS

Ultimately, it is crucial to understand what legislative guidance and trends mean for companies, consumers, and regulators, and how this will or should impact their behaviors.

A. Companies

The most crucial aspect for companies is to understand what liability schemes are in place so they can perform a cost-benefit analysis before developing AI products. Depending on what liability a product may fall under, a company's analysis may change on whether a certain product is worthwhile to pursue.

Companies must be aware of potential risks posed by AI, specifically risks relating to bias and discrimination.[226] Regulators are concerned that "continuous learning could cause algorithms to discriminate or become unsafe in new, hard-to-detect ways."[227] Companies will need to learn from previous mistakes and protect themselves against AI performing in unexpected ways. In examples such as Microsoft and its "Tay" chatbot, companies will need to develop plans on how to ensure their AI powered devices will not react in unexpected, problematic ways.

Some companies, including Google, Microsoft, and BMW, are already crafting "formal AI policies with commitments to safety, fairness, diversity, and privacy."[228] Other companies have taken the initiative to appoint "chief ethics officers to oversee the introduction and enforcement" of formal AI policies and support these policies with ethics governance boards.[229]

Even companies that do not sell AI products must be aware of the AI chosen to assist in running their companies—for instance, what hiring technology is being used. Employers must choose hiring technologies that do not impact people with disabilities as the use of a hiring technology

225. Korinek, *supra* note 219.
226. Kelly et. al., *supra* note178.
227. Candelon et. al., *supra* note 88.
228. *Id.*
229. *Id.*

could lead to unlawful discrimination.[230] Companies should be aware of hiring technologies that "try to predict who will be a good employee by comparing applicants to current successful employees," which may result in discrimination against those with disabilities they may not be a person with a disability currently on staff.[231]

There is undoubtedly "more stringent AI regulations that are on the horizon (at least in Europe and the United States)," and companies must be prepared to equip themselves with new data protocols, diversity awareness training, AI monitoring protocols,[232] and potentially, insurance for AI systems.[233] Automated systems have the potential to "invisib[ly] replicate historical discrimination and bias" or "promulgate other unfair treatment."[234] Therefore, companies must be prepared to mitigate this risk. Mitigation could "involve increasing human input in the AI process or making use of open-source bias mitigation tools."[235] In response to regulatory guidance, companies should craft specific Terms of Use with guidelines influenced by how regulatory bodies and peer companies are managing potential risks associated with AI.[236] Companies may want to consider developing an enforcement program based on their product, which may include "account restrictions, pre-litigation outreach, and appropriate escalation to civil litigation as needed."[237]

Companies should also consider whether their warning labels are evolving at the same rates as their technology. A good warning "can ameliorate [risks] by helping to change human behavior to reduce the likelihood of accidents."[238] Thus, the riskier an AI product is, "the greater the need for attention-grabbing warnings."[239] Companies must also consider warning

---

230. U.S. Dep't of Just. – C. R. Div., Algorithms, Artificial Intelligence, and Disability Discrimination in Hiring 2, https://beta.ada.gov/assets/_pdfs/ai-guidance.pdf [https://perma.cc/5MWP-58TU].

231. *Id.* at 2–3.

232. Candelon et. al., *supra* note 88.

233. Kalra, *supra* note 4, at 15; *see* Gupta, *supra* note 6, at 6079 ("For this, developers may be required by law to take out insurance to compensate people harmed by Al when no other person is legally responsible for the damage. Law must come up with a way to hold the autonomous mechanisms liable in the near future for their doings.").

234. Robert Wennagel, *Dark Systems: Reprogramming Artificial Intelligence Regulations to Promote Fairness and Employment Nondiscrimination*, 39 SANTA CLARA HIGH TECH. L.J. 1, 6–7 (2022).

235. Kelly et. al., *supra* note 178.

236. *See* Erin M. Bosman et. al., *Deepfake Litigation Risks: The Collision of AI's Machine Learning and Manipulation,* 4 J. ROBOTICS, A.I. & L. 261, 265 (2021).

237. *Id.*

238. William D. Kennedy et al., *Making Safer Robotic Devices,* 4 J. ROBOTICS, A.I. & L. 283, 284 (2021).

239. *Id.* at 285.

about risks "associated with both proper and even reasonably foreseeable improper usage" of the device.[240]

One of the most effective, potential solutions to combat the numerous problems with imposing a strict liability scheme and combatting the lack of uniform regulations is a form of third-party insurance for AI-related harms.[241] There have already been a handful of companies who have begun turning to insurance providers for other risks related to IoT, specifically, the cyber security risks. Insurance for cyber risks are likely to reach "global premiums being on the order of $20 billion by 2025."[242] For example, the department store chain Target utilizes insurance for cyber security of IoT and "was able to recover $44 million from its insurance carrier following its massive data breach in 2013-2014."[243] Insurance will likely expand beyond cyber risks, and "developers may be required by law to take out insurance to compensate people harmed by AI when no other person is legally responsible for the damage."[244]

In the U.S., the medical field has already begun recommending third-party insurance providers to companies for AI-related harms. It has been proposed that "all robotic surgeons should be independently insured with equal contributions from all actors in the making of the machine, which would cover the damages, if and when necessary."[245] The Medical Devices Regulation is a sector-specific legislation that states that "medical device manufacturers are liable for all claims arising from their product and must be prepared to provide sufficient financial coverage in respect of their liability."[246] This is achieved in practice "through adequate liability insurance for covering no-fault liability."[247]

The European Parliament's recent proposal for a regulation on liability for AI proposed strict liability backed by mandatory insurance for high-

240. *Id.*
241. Scott J. Shackelford & Scott O. Bradner, *Have You Updated Your Toaster? Transatlantic Approaches to Governing the Internet of Everything*, 72 HASTINGS L. J. 627, 636 (2021).
242. *Id.*
243. *Id.*
244. Gupta, *supra* note 6, at 6079.
245. Kalra, *supra* note 4, at 15.
246. Beatrice Schutte & Lotta Majewski, *Private Liability for AI-Related Harm: Towards More Predictable Rules for the Single Market*, 6 MKT & COMPETITION L. REV 123, 128 (2022).
247. *Id.*

risk autonomous AI products.[248] Third-party insurance could "transform the risk associated with the service it offers into a predictable cost of its activity."[249] This type of insurance would create consumer confidence in the market while strengthening and consolidating uncertain regulatory laws.[250]

B. Consumers

A "personal risk-return calculus" will likely determine consumer's "attitudes toward evolving AI."[251] Consumers will need to educate themselves on both the benefits and the drawbacks of both AI and connected devices before calculating their willingness to assume these risks. Additionally, consumers will have to grapple with is the delineation away from a one-dimensional transaction to the multi-dimensional transactions which could be the cornerstone of smart device purchases in the future. When a consumer buys a "regular non smart fridge, printer, car, soft toy or electric toothbrush, the transaction is relatively straight forward and one dimensional."[252] In this transaction, the consumer is paying face-value for the product, eliminating underlying gains a company could receive for the transaction. However, smart device transactions are completely different. Smart devices "collect data and communicate with consumers," which can create "new funding opportunities," for companies.[253] Consumers must decide whether they are willing to "sacrifice data and accep[t] advertising messages," in exchange for the services provided by smart devices.[254]

C. Regulators

The biggest strides that will need to come for AI liability in the future generally involve regulatory laws. Many agencies have already proposed frameworks that will help define the scope of liability, including an ethical framework and an AI Bill of Rights. Regulators must be aware of these proposals and work towards creating a uniform regulation between agencies. A key part of creating these frameworks will be to ensure that humans remain in control and take steps "to ensure appropriate safeguards

248. *See* Resolution of 20 October 2020 with Recommendations to the Commission on a Civil Liability Regime for Artificial Intelligence, EUR. PARL. DOC. P9_TA (2020).
249. Luigi Buonanno, *Civil Liability in The Era of New Technology: The Influence of Blockchain*, EURO. L. INST., 1, 13 (Sept. 1. 2019).
250. *Id.*
251. Candelon et. al., *supra* note 88.
252. Tokeley, *supra* note 22, at 124.
253. *Id.*
254. *Id.*

are implemented to mitigate both intended and unintended consequences" of AI.[255]

As no current agency has the capacity to manage growing AI regulations, there will likely have to be a new agency entirely dedicated to AI regulations and that agency would have to conduct independent evaluations of AI across various products and services.

VII. CONCLUSION

As AI technology continues to advance rapidly, establishing a new model for AI regulation will be crucial to protect both companies and consumers. The U.S. must consider consumer safety as well as innovation-conducive policies when assigning liability to AI. By using EU regulatory guidance as a starting point, this paper argues that a multi-tiered liability scheme coupled with a Uniform AI ethical framework and the creation of an independent AI regulatory agency would aid the U.S. in striking the right balance to effectively combat the risks posed by AI and IoT.

255. ACT-IAC, ARTIFICIAL INTELLIGENCE/MACHINE LEARNING PRIMER 23 (Mar. 12, 2019), https://www.actiac.org/system/files/Artificial%20Intelligence%20Machine%20Learning%20Primer.pdf [https://perma.cc/8HPJ-XXDU].