IS YOUR USE OF AI VIOLATING THE LAW? AN OVERVIEW OF THE CURRENT LEGAL LANDSCAPE

*Miriam Vogel**
*Michael Chertoff***
Jim Wiley†
Rebecca Kahn‡

As AI adoption expands, so does the landscape of related legal liability. Lawyers, policymakers, and business executives should become AI-literate with respect to the potential harms and litigation risks associated with this technology as it grows in capabilities and adoption. This Article provides a brief introduction to the legal landscape to consider when developing, licensing, or using AI systems. While the regulatory and legal landscapes are rapidly evolving, this Article aims to provide a foundational understanding to help mitigate liability and avoid the associated harms to companies, individuals, and communities.

Introduction

Artificial intelligence ("AI") is increasingly becoming a fundamental component of daily activities. It is already used in highly consequential applications, including in school districts,[1] hospitals,[2] child

1. Security Staff, *Pennsylvania school district uses AI-based gun detection*, Sec. Mag. (Nov. 3, 2022), https://www.securitymagazine.com/articles/98570-pennsylvania-school-district-uses-ai-based-gun-detection [https://perma.cc/L8UY-5BR8].

2. Terence Mills, *AI For Health And Hope: How Machine Learning Is Being Used In Hospitals*, Forbes (Feb. 18, 2022, 3:42 AM), https://www.forbes.com/sites/forbestechcouncil/2022/02/16/ai-for-health-and-hope-how-machine-learning-is-being-used-in-hospitals/?sh=7600bee755be [https://perma.cc/8XNM-NBU7].

welfare systems,[3] and police departments.[4] These uses—from hiring, to housing, to Medicaid benefits—can and do have a significant impact on the lives of individuals, families, and communities.[5] Generative AI offers a new realm of applications and efficiencies—some productive, such as brainstorming assistance and improving business systems,[6] while other uses are more nefarious and harmful, such as enabling cybercrime and fraudulent schemes.[7] As a result, all AI actors,[8] including those building, buying, licensing, and deploying these systems, must consider their own potential legal liability.

Understanding how and where AI intersects with the law is increasingly good practice for senior executives and critical for competent legal counsel. As reliance on AI has increased, so too has AI-based litigation in courts across the United States and abroad. The Stanford AI Index Report identified over 100 AI-related legal cases in the U.S. in 2022—6.5 times more than in 2016.[9] These cases covered a

3. Anjana Samant et al., *Family Surveillance by Algorithm: The Rapidly Spreading Tools Few Have Heard Of*, Am. Civ. Liberties Union (Sept. 29, 2021), https://www.aclu.org/news/womens-rights/family-surveillance-by-algorithm-the-rapidly-spreading-tools-few-have-heard-of [https://perma.cc/545D-WNF5].

4. Karen Hao, *AI is sending people to jail—and getting it wrong*, MIT Tech. Rev. (Jan. 21, 2019), https://www.technologyreview.com/2019/01/21/137783/algorithms-criminal-justice-ai/ [https://www.perma.cc/F9WY-QFBQ].

5. Erin Denniston Leach, *Beware of the Use of Artificial Intelligence Recruitment and Hiring Tools*, Snell & Wilmer (May 18, 2022), https://blog.swlaw.com/labor-and-employment/2022/05/18/beware-of-the-use-of-artificial-intelligence-recruitment-and-hiring-tools/ [https://perma.cc/WA44-RBU2] (hiring); *Meta (Facebook) Settles Fair Housing Violation Allegations*, Nat'l Ass'n of Realtors (Dec. 28, 2022), https://www.nar.realtor/legal-case-summaries/meta-facebook-settles-fair-housing-violation-allegations [https://perma.cc/GL4W-Q9GG] (housing); Hannah Bloch-Wehba, *Access to Algorithms*, 88 Fordham L. Rev. 1265 (2020), https://ir.lawnet.fordham.edu/flr/vol88/iss4/2 [https://perma.cc/3TP8-UDP6] (Medicaid benefits).

6. Tojin T. Eapen at al., *How Generative AI Can Augment Human Creativity*, Harv. Bus. Rev. (July–Aug. 2023), https://hbr.org/2023/07/how-generative-ai-can-augment-human-creativity [https://perma.cc/WLT8-BD69] (fueling creativity); Michael Chui et al., McKinsey & Co., The economic potential of generative AI: The next productivity frontier (2023), https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier#introduction [https://perma.cc/C956-S63N] (improving business systems).

7. Thomas Brewster, *Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find*, Forbes (May 2, 2023, 8:37 AM), https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/ [https://perma.cc/GE26-RMC4].

8. *AI Risk Management Framework*, Nat'l Inst. of Standards & Tech., U.S. Dep't of Com. (2024), https://www.nist.gov/itl/ai-risk-management-framework [https://perma.cc/RUK7-J398] ppg 35–37.

9. Stan. Univ. Hum.-Centered A.I., Artificial Intelligence Index Report 2023 (2023), https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf [https://perma.cc/25JP-U442].

wide range of sectors, from financial and professional services to health care, transportation, media, oil and gas, and others.[10] Similarly, the bases of these legal claims span across torts and contract law to constitutional, corporate, criminal, and intellectual property.[11]

This Article provides an introduction to help recognize AI-related liability before it becomes harmful or costly. The authors recognize the inherent limitations of this Article: it is not an exhaustive analysis nor complete list of applicable laws and regulations, but rather an introduction to the current legal implications of AI use. The Article starts with a brief description of AI and the professional responsibilities of lawyers, followed by an overview of laws and policies related to AI, in consumer protection, civil rights and criminal justice, privacy, intellectual property, contracts, and AI readiness and national security, including emerging, cross-sectoral AI reform proposals in Congress, the Executive Branch, and state and local governments. It concludes with a brief overview of global AI laws.

Although often perceived to be a new concept, the term "artificial intelligence" was first coined more than half a century ago. In 1956, John McCarthy organized a group of scientists for the Dartmouth Summer Research Project on Artificial Intelligence.[12] In the sixty-five years since, AI has burgeoned into a multibillion-dollar global market.

The adoption of AI has more than doubled in the last five years, and yet there is not been consensus on its definition.[13] Fortunately, intergovernmental entities,[14] U.S. federal agencies,[15] academic institutions,[16] and others have increasingly worked toward aligning definitions. In January 2023, the National Institute of Standards and Technology ("NIST") set forth a now well-accepted definition of AI

10. *Id.*

11. *Id.*

12. *Artificial Intelligence Coined at Dartmouth*, DARTMOUTH COLL., https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth [https://perma.cc/PPC3-UN7Z].

13. CHUI, *supra* note 8.

14. OECD, *OECD AI Principles Overview*, OECD.AI POLICY OBSERVATORY, https://oecd.ai/en/ai-principles [https://perma.cc/A68X-PJH5].

15. *Information Technology: Artificial Intelligence Overview*, NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COM., https://www.nist.gov/artificial-intelligence [https://perma.cc/4CXV-EBYL].

16. STAN. UNIV. HUM.-CENTERED A.I., ARTIFICIAL INTELLIGENCE DEFINITIONS, https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf [https://www.perma.cc/2432-GTBQ].

in its congressionally-mandated AI Risk Management Framework ("AI RMF"), adapted from an earlier definition proposed by the Organisation for Economic Cooperation and Development ("OECD").[17] The NIST definition provides: "An AI system is an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy."[18] In essence, AI is a broad field of technologies that uses algorithms, data, and computational power to simulate human intelligence.

It is helpful to understand that AI is not a singular technology, but rather a collection of them. A few types of AI technologies include speech recognition, deep learning, natural language generation, and machine learning.[19] Machine learning utilizes training data, which is the information used to teach the model. This data is fed into the machine learning model, enabling it to learn, identify patterns, and make predictions.[20]

Machine learning has expanded in recent years due to increased access to data,[21] compute power,[22] and hardware efficiency.[23] The most complex forms of machine learning involve deep learning, or neural networks, modeled after the human brain, comprising thousands or even millions of interconnected processing nodes.[24] This technology enables machines to analyze data, learn from it, make decisions, and perform

17. Nat'l Inst. of Standards & Tech., U.S. Dep't of Com., Artificial Intelligence Risk Management Framework (2023) [hereinafter AI RMF 1.0], https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf [https://perma.cc/8P6Q-ES7C].

18. AI RMF 1.0, *supra* note 17.

19. *What Are The Different Types of AI?*, Microsoft 365 (June 12, 2023), https://www.microsoft.com/en-us/microsoft-365-life-hacks/writing/what-are-the-different-types-of-ai [https://perma.cc/AAG2-NE5J].

20. Sara Brown, *Machine learning, explained*, MIT Sloan Sch. of Mgmt. (Apr. 21, 2021), https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained [https://perma.cc/BX98-L9HT].

21. Sage Lazzaro, *Machine learning's rise, applications, and challenges*, VentureBeat (June 21, 2021, 6:21 AM), https://venturebeat.com/ai/machine-learnings-rise-applications-and-challenges/.

22. Andrew Lohn & Micah Musser, *AI and Compute: How Much Longer Can Computing Power Drive Artificial Intelligence Progress?*, Ctr. for Sec. & Emerging Tech. (Jan. 2022), https://cset.georgetown.edu/publication/ai-and-compute/ [https://perma.cc/2LCM-YWM4].

23. Adam Zewe, *New hardware offers faster computation for artificial intelligence, with much less energy*, MIT News Off. (July 28, 2022), https://news.mit.edu/2022/analog-deep-learning-ai-computing-0728 [https://perma.cc/3H3A-HCES].

24. Brown, *supra* note 20.

actions that mimic human cognitive functions such as problem-solving, reasoning, and learning.

One of the more advanced forms of AI is generative AI, the technology that powers ChatGPT, released by OpenAI and incorporated in Microsoft's Bing; Google's Bard; and Anthropic's Claude. Generative AI systems use neural networks to identify the patterns and structures within existing data to generate new and original content.[25] This technology presents innumerable novel and innovative applications, from generating images and synthetic data to developing content ideas and text.[26] However, it can also generate false and even malicious content capable of perpetuating harm.[27] This is an area of increased potential legal liability and uncertainty,[28] particularly when AI is used to support infrastructure or interact directly with downstream users.

When working with AI systems or advising clients on potential liability, it is helpful to consider that every human touch point—from designing the model to enable an AI-enabled solution to constructing the use cases or populations in the testing phase(s)—is a potential point of harm introduction, such as bias, that can impact outcomes.[29] AI is trained on enormous amounts of data, which generally are records of human discussions and interactions (e.g., Reddit discussions, social media comments, financial determinations and government records). As such, they will reflect biases and limitations such as historical incidence

25. Aldeida Aleti, *Software Testing of Generative AI Systems: Challenges and Opportunities*, Cornell Univ. arXiv (Sept. 11, 2023), https://arxiv.org/abs/2309.03554 [https://perma.cc/6P2P-HQUE] (discussing the capabilities of Generative AI systems, including their use of neural networks to understand and recreate patterns from large amounts of data).

26. Forbes Councils Member Expert Panel, *15 Surprising Ways Industries May Soon Leverage Generative AI*, Forbes (May 25, 2023, 8:15 AM), https://www.forbes.com/sites/forbestechcouncil/2023/05/25/15-surprising-ways-industries-may-soon-leverage-generative-ai/ [https://perma.cc/4MHB-FLGS] (generating images and synthetic data); *Artificial Intelligence: Generative AI*, BCG, https://www.forbes.com/sites/forbestechcouncil/2023/05/25/15-surprising-ways-industries-may-soon-leverage-generative-ai/ (generating content ideas and text to spur creativity).

27. Tiffany Hsu & Stuart A. Thompson, *Disinformation Researchers Raise Alarms About A.I. Chatbots*, N.Y. Times (Feb. 8, 2023), https://www.nytimes.com/2023/02/08/technology/ai-chatbots-disinformation.html (false content); Michael Atleson, *Chatbots, deepfakes, and voice clones: AI deception for sale*, Fed. Trade Comm'n: Bus. Blog (Mar. 20, 2023), https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale [https://perma.cc/WDD6-MKDJ] (malicious content).

28. Model Rules of Pro. Conduct r. 1.2(d) (Am. Bar Ass'n 1983).

29. Cathy O'Neil, *Do Algorithms Perpetuate Human Bias*, NPR/TED Radio Hour (Jan. 26, 2018, 9:12 AM), https://www.npr.org/2018/01/26/580617998/cathy-oneil-do-algorithms-perpetuate-human-bias [https://perma.cc/F332-D2FN].

of discrimination.[30] For example, one study found that, compared to white applicants, Black applicants were 80 percent more likely to be denied a mortgage by an algorithm raising concerns of redlining and other forms of bias contained in training data.[31] Another study revealed that an algorithm, compounded with historical bias in care that was captured in training data, was used to determine whether patients required additional care, and resulted in patients receiving lesser care based on their race and class.[32] An AI recruiting tool was abandoned by a major tech company after significant time and investment because its propensity for gender bias could not be remedied, once again, likely based on biases in the training data that were learned by and embedded in the AI system.[33]

Rule 1.1 of the American Bar Association ("ABA") Model Rules provides that competent legal representation "requires legal knowledge, skill, thoroughness and preparation."[34] How does this obligation relate to AI technology? According to comment eight of the rule, "To maintain the requisite level of knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the *benefits and risks associated with relevant technology*" (emphasis added).[35] As of April 2023, 39 jurisdictions from Alaska to Wyoming have adopted a statement on technology competence.[36]

Resolution 112, adopted by the ABA House of Delegates in August 2019, urged courts and lawyers to address the ethical and legal

30. AI experts have grappled with how society can best reduce the human biases that are reflected in artificial intelligence systems. *See., e.g.*, James Manyika, Jake Silberg, & Brittany Presten, *What Do We Do About the Biases in AI?*, Harvard Business Review (Oct. 25, 2019), https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai [https://perma.cc/Z89V-V3FR].

31. Emmanuel Martinez & Lauren Kirchner, *The secret bias hidden in mortgage-approval algorithms*, AP News (Aug. 25, 2021, 12:04 PM), https://apnews.com/article/lifestyle-technology-business-race-and-ethnicity-mortgages-2d3d40d5751f933a88c1e17063657586 [https://perma.cc/8VX6-4JQH]; Newsroom, Consumer Fin. Prot. Bureau, Director Chopra's Prepared Remarks on the Interagency Enforcement Policy Statement on "Artificial Intelligence" (Apr. 25, 2023), https://www.consumerfinance.gov/about-us/newsroom/director-chopra-prepared-remarks-on-interagency-enforcement-policy-statement-artificial-intelligence/ [https://perma.cc/8V7V-WDWC].

32. Ziad Obermeyer et al., *Dissecting racial bias in an algorithm used to manage the health of populations*, Sci., October 2019, at 447–453.

33. Jeffrey Dastin, *Amazon scraps secret AI recruiting tool that showed bias against women*, Reuters (Oct. 9, 2012, 11:00 PM), https://www.reuters.com/article/idUSL2N1VB1FQ/.

34. Model Rules of Pro. Conduct r. 1.1 (Am. Bar Ass'n 1983).

35. Model Rules of Pro. Conduct r. 1.1 cmt. 8 (Am. Bar Ass'n 1983).

36. *Id.*

ramifications of utilizing AI.[37] The resolution underscores that, in order to provide sound counsel to clients, lawyers must consider how bias and transparency requirements can create risk for AI users.[38]

Two years after adopting Resolution 112, the House of Delegates adopted Resolution 604 to address how attorneys, regulators, and other stakeholders assess AI in the legal realm, emphasizing principles such as accountability, transparency, and traceability.[39] The resolution underscores that "individual and enterprise accountability and human authority, oversight, and control are required and it is not appropriate to shift legal responsibility to a computer or an 'algorithm' rather than to responsible people and other legal entities." In other words, the use of AI does not help evade liability and, to the contrary, may establish a violation of this standard.

Accordingly, the resolution called for all organizations who design, develop, and deploy AI to maintain human authority; be accountable for their AI uses; ensure traceability and transparency; and instill practices for documentation of key decisions regarding design and risk of their AI.

In short, the use of AI does not preclude, and could at times invite, legal liability. As such, lawyers and executives should investigate and understand how companies, clients and employees are using AI, and the implications of its use, in order to avoid unexpected legal liability. Judges will also need to understand the legal implications of AI to properly adjudicate the growing number of AI claims in their courtrooms. The Article now turns to a series of current legal frameworks that may be applicable to AI use. The subsequent sections of this Article examine the application of AI to traditional areas of law, including consumer protection concerns, civil rights and criminal justice, intellectual property, contracts, privacy, AI readiness and policy proposals, and global considerations.

37. Am. Bar Ass'n, Annual Meeting Resolution 112 (Aug. 2019).

38. *Id.*

39. *Midyear Meeting 2023 – House of Delegates Resolution 604*, Am. Bar Ass'n, https://www.americanbar.org/news/reporter_resources/midyear-meeting-2023/house-of-delegates-resolutions/604/; Amanda Robert, *ABA House adopts3 guidelines to improve use of artificial intelligence*, ABAJournal (Feb. 6, 2023, 11:22 AM), https://www.abajournal.com/web/article/aba-house-adopts-3-guidelines-to-improve-use-of-artificial-intelligence [https://perma.cc/8UGN-PCSQ].

I. Consumer Protection Concerns

"AI does not, today, exist in a law-free environment."
— FTC Commissioner Alvaro M. Bedoya[40]

Whether developing, licensing, using, or deploying AI, organizations could be at risk for liability under current consumer protection laws. In a historic joint statement released on April 25, 2023, senior officials from the Civil Rights Division of the U.S. Department of Justice ("DOJ"), the Federal Trade Commission ("FTC"), the Consumer Financial Protection Bureau ("CFPB"), and the U.S. Equal Employment Opportunity Commission ("EEOC") highlighted their enforcement capabilities—and intent—"to protect the public from bias in automated systems" and AI with their collective authorities.[41]

Contrary to the "myth" that AI is unregulated, FTC Commissioner Alvaro M. Bedoya clarified, "the reality is, AI is regulated."[42] This section highlights how enforcement bodies such as the FTC, CFPB, and the Security Exchange Commission ("SEC"), together with legislatures and elected officials, are planning to apply traditional consumer protection laws to address deceptive, discriminatory, fraudulent, and harmful practices involving AI systems, as well as developing additional legal tools to regulate AI and protect consumers.

This section will describe the following issues: (1) deceptive and unfair practices, including the FTC and CFPB's roles in regulating unfair and deceptive business practices related to AI, the FTC's authority under Section 5 of the FTC Act to act against unfair or deceptive acts or practices, and the CFPB's independent actions under its authority to tackle unfair practices; (2) deepfakes and fraud, including the FTC's efforts to regulate fraudulent AI products and the rise of sophisticated deepfakes, and legal challenges and the proposed bills to manage deepfake technology and its implications, especially concerning U.S. elections; (3) AI-related torts, including discussion on how AI could change liability norms, especially in the context of self-driving cars and AI in medical devices, and an exploration of traditional and potential

40. Commissioner Alvaro M. Bedoya, Fed. Trade Comm'n, Remarks Before the International Association of Privacy Professionals: Early Thoughts on Generative AI (Apr. 5, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/Early-Thoughts-on-Generative-AI-FINAL-WITH-IMAGES.pdf [https://perma.cc/77N8-3MHK].

41. Rohit Chopra et al., *Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems*, Fed. Trade Comm'n, https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf [https://perma.cc/RMN5-6MAB].

42. Bedoya, *supra* note 40.

new liability schemes applicable to AI; (4) AI-related product liability, including the evolving landscape of the law and challenges in litigating these cases; and (5) future regulatory frameworks and enforcement, including the FTC's and SEC's ongoing and proposed regulatory efforts to address AI's challenges, and the potential for new rules and frameworks to guide the development and deployment of AI in various sectors.

A. Deceptive and Unfair Practices

Consumer protection agencies have announced their intent to use current legal authorities to address harms emerging from AI development, use, and deployment. For instance, the FTC and CFPB regulate various forms of unfair and deceptive business practices, and clarified that this includes false or bolstered claims about AI products.[43]

Section 5 of the FTC Act is one legal tool at their disposal. This provision endows the FTC with the authority to regulate unfair or deceptive acts or practices ("UDAP") in or affecting commerce, including companies making, selling, or using AI.[44] Simply put, if a company makes deceptive claims using or about AI, or injures a consumer in a way that satisfies the FTC test for unfairness, that company could be in violation of this act.[45]

In addition to the joint agency statement noted above, the CFPB independently announced that it would act to curb "unfair" practices under its own statutory power.[46] CFPB Director Rohit Chopra explained that "certain discriminatory practices may . . . trigger liability under the

43. Rebecca Kelly Slaughter et al., *Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission*, YALE J. OF L. & TECH. (Aug. 2021), https://law.yale.edu/sites/default/files/area/center/isp/documents/algorithms_and_economic_justice_master_final.pdf [https://perma.cc/6ARC-U5S7]; Elisa Jillson, *Aiming for Truth, fairness, and equity in your company's use of AI*, FED. TRADE COMM'N BUS. BLOG (Apr. 19, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai [https://perma.cc/42WB-X7HS].

44. FED. TRADE COMM'N, A BRIEF OVERVIEW OF THE FEDERAL TRADE COMMISSION'S INVESTIGATIVE, LAW ENFORCEMENT, AND RULEMAKING AUTHORITY (May 2021), https://www.ftc.gov/about-ftc/mission/enforcement-authority [https://perma.cc/9GTZ-284V]; 15 U.S.C. § 45 (2018).

45. Bedoya, *supra* note 40.

46. Newsroom, Consumer Fin. Prot. Bureau, CFPB Targets Unfair Discrimination in Consumer Finance (Mar. 16, 2023), https://www.consumerfinance.gov/about-us/newsroom/cfpb-targets-unfair-discrimination-in-consumer-finance/ [https://perma.cc/F2TL-BMG8].

Consumer Financial Protection Act ("CFPA"), which prohibits unfair, deceptive and abusive acts and practices ("UDAPs")."[47]

In a blog post from February 2023,[48] the FTC warned companies to "keep your AI claims in check" to avoid UDAP violations.[49] The post urges companies to refrain from exaggerating their AI products' capabilities, including falsely asserting that AI solutions are superior to non-AI solutions, failing to address reasonably foreseeable risks, and making baseless claims about whether a product uses AI.[50]

In addition to harmful claims about AI, UDAP provisions also allow regulators to curb unfair business practices. Another FTC blog post underscores that the agency relies on "decades" of enforcement experience to inform its decisions when applying Section 5 authority to AI.[51] The FTC accordingly follows precedent to target the sale of racially biased algorithms in addition to deceptive exaggerations of the power, efficacy, or unbiased nature of models. The FTC also warns that AI products that are likely to cause substantial injury without countervailing benefits will be deemed unfair.[52] Two enforcement actions and one Civil Investigative Demand ("CID"), discussed below, are examples of how the FTC exercises its power to address deceptive and unfair practices and enforce consent orders.

In a 2021 complaint, the FTC alleged that Everalbum, a company offering photo storage and organization services, deceived its users by (1) misrepresenting users' ability to control the company's facial recognition feature; and (2) retaining users' media even after they deactivated their accounts indefinitely, despite promises to delete.[53] In the settlement order, the FTC instructed Everalbum not to misrepresent its practices, to acquire the consent of its users before using facial recognition technology, but to delete the data it had collected, and to delete algorithms and models developed using the images and videos of its users.[54] This last requirement of "algorithmic disgorgement"[55] is

47. Consumer Fin. Prot. Bureau, Laws and Regulations: UDAAP, https://files.consumerfinance.gov/f/documents/cfpb_unfair-deceptive-abusive-acts-practices-udaaps_procedures_2023-09.pdf [https://perma.cc/HN5X-QFNZ].

48. Michael Atleson, *Keep your AI claims in check*, Fed. Trade Comm'n Bus. Blog (Feb. 27, 2023), https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check [https://perma.cc/E6GU-VFNL].

49. *See* Jillson, *supra* note 43.

50. *See id.*

51. *Id.*; FTC Commissioner Rebecca Kelly Slaughter provides a thorough examination of FTC enforcement of AI *in* Slaughter, *supra* note 43.

52. Jillson, *supra* note 43.

53. Decision and Order, In re Everalbum, Inc., No. C-4743 (F.T.C. May 6, 2021).

54. *Id.*

55. Slaughter, *supra* note 43.

an example of FTC authority to "order relief reasonably tailored to the violation of the law"[56] to remediate and deter AI harms.[57]

The FTC 2019 complaint against Facebook presents another illustrative case[58] in which the agency alleged that the social media company misled its users by indicating they could opt out of the facial recognition program when its program was using its users' photos by default.[59] The FTC and Facebook ultimately settled on a historic $5 billion civil penalty and instituted an amended consent order that could be enforced by the FTC or DOJ.[60]

In July 2023, OpenAI became the latest large tech company to come under an FTC investigation.[61] Using its 15 U.S.C. § 45 Section 5 authority, the FTC issued a civil investigative demand ("CID") requesting information about the company's products, customers, and privacy and data security policies and procedures. The goal was to determine whether the company had engaged in unfair or deceptive practices.[62] The CID sought information such as the model development and training procedures for its large language model ("LLM") products, including specifics on how personal information is handled, as well as its disclosures and risk assessment and mitigation processes. Through mechanisms such as CIDs, the FTC and other regulators[63] have tools and authorities to demand greater transparency and honest representations from AI developers.

---

56. *Id.* at 39.

57. Avi Gesser et al., *Model Destruction – The FTC's Powerful New Al and Privacy Enforcement Tool*, Compliance & Enf't (Mar. 30, 2022), https://wp.nyu.edu/compliance_enforcement/2022/03/30/model-destruction-the-ftcs-powerful-new-ai-and-privacy-enforcement-tool/ [https://perma.cc/S4UM-VVUD].

58. Complaint, United States v. Facebook, Inc., No. 19-cv-2184 (D.D.C. July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf [https://perma.cc/4SAA-FAM8].

59. Jillson, *supra* note 43.

60. Plaintiff's Consent Motion for Entry of Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief and Memorandum in Support, United States v. Facebook, Inc., No. 19-cv-2184 (D.D.C. July 24, 2019); Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2024), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook [https://perma.cc/49QV-KE3E].

61. David Hamilton, *FTC investigating ChatGPT creator OpenAI over consumer protection issues*, AP News (July 13, 2023), https://apnews.com/article/openai-chatgpt-investigation-federal-ftc-76c6218c506996942282d7f5d608088e [https://perma.cc/SWK2-BQN8].

62. Civil Investigative Demand Schedule, Fed. Trade Comm'n, FTC File No. 232-3044, https://www.washingtonpost.com/documents/67a7081c-c770-4f05-a39e-9d02117e50e8.pdf?itid=lk_inline_manual_4.

63. Antitrust Civil Process Act, 15 U.S.C. §§ 1311–1314.

B. Deepfakes and Fraud

Recent developments in generative AI make it easier than ever to create deepfake videos,[64] voice clones, and false information that can be used in numerous illicit or deceitful ways—from extortion or imposter scams, to generating spear-phishing emails and creating content and personas, to disseminating false information and fake news.[65]

AI can increase security risks and falsifications, from creating personalized email spam to impersonating an individual's voice to access a loved one's, bank account after training on just three seconds of audio.[66] Reports from security companies and research organizations warn of the increased accessibility and growing sophistication of AI-powered fraud.[67] A recent Center for Security and Emerging Technology ("CSET") study outlines how advancing readily available LLM technology can increase the number of people who can engage in deceptive propaganda—at a larger scale, lower cost, and individualized to a target.[68] Moreover, as disinformation advances, it is less likely than previous scams to be detected as false or fake, thereby increasing the perceived credibility and persuasiveness of the false content.

A violation of the FTC Act may occur "if you make, sell, or use a tool that is *effectively designed to deceive—even if that's not its intended or sole purpose*" (emphasis added).[69] Accordingly, the FTC states that companies considering using or selling AI products should consider whether they should make or sell generated content, whether risks are effectively mitigated, whether they are overly reliant on post-release detection, and whether they are misleading people about the

64. Deepfake is "an image or recording that has been convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said." *Deepfake*, Merriam-Webster, https://www.merriam-webster.com/dictionary/deepfake (last visited May 7, 2024).

65. Atleson, *supra* note 48.

66. Andrew Patel & Jason Sattler, WithSecure Intelligence, Creatively malicious prompt engineering (Jan. 2023), https://labs.withsecure.com/content/dam/labs/docs/WithSecure-Creatively-malicious-prompt-engineering.pdf (personalized email spam); Benj Edwards, *Microsoft's new AI can simulate anyone's voice with 3 seconds of audio,* Ars Technica (Jan. 9, 2023), https://arstechnica.com/information-technology/2023/01/microsofts-new-ai-can-simulate-anyones-voice-with-3-seconds-of-audio/ (3 seconds of radio).

67. Patel & Sattler, *supra* note 66; Josh A. Goldstein et al., *Forecasting Potential Misuses of Language Models for Disinformation Campaigns—and How to Reduce Risk,* Ctr. for Sec. & Emerging Tech. (Jan. 2023), https://cset.georgetown.edu/article/forecasting-potential-misuses-of-language-models-for-disinformation-campaigns-and-how-to-reduce-risk/ [https://perma.cc/U6BF-656U].

68. Goldstein *supra* note 67.

69. Atleson, *supra* note 48.

nature of the content they are consuming.[70] In testimony before the House Committee on Energy and Commerce, FTC Chair Lina Khan pointed out that AI has been used to "turbocharge frauds and scams," which can leave market participants "on the hook for FTC action."[71] The examples below demonstrate how AI technology can be harnessed to perpetrate fraud and violate the FTC Act's prohibition on deceptive or unfair conduct.[72]

Examples of AI-enabled fraud are already evident. In 2021, AI "deep voice" technology facilitated the impersonation of a CEO's voice, which was used to steal $35 million from a Japanese company in Hong Kong.[73] In 2022, the FBI warned that an actor using AI stole personally identifiable information ("PII") during the job application process, employing techniques such as spoofing and deepfakes to impersonate others.[74] Following these events, in March 2023, an advanced version of the Generative Pre-trained Transformer series developed by OpenAI, GPT-4 convinced a Task Rabbit worker to complete a Completely Automated Public Turing to tell Computers and Humans Apart ("CAPTCHA") test on its behalf to "verify" the AI was a human by claiming it was a visually impaired individual.[75]

Deepfakes have already started to perpetuate the spread of misinformation with significant consequences. In one incident in February of 2023, deepfake audio and videos were used to deceptively portray[76] Joe Rogan, Emma Watson, and other celebrities as purportedly endorsing products and making falsified racist and sexist statements. Another highly consequential deepfake incident involved the use of

---

70. *Id.*

71. The Comm. on Energy & Com., *IDC Subcommittee Hearing: "Fiscal Year 2024 Federal Trade Commission Budget"*, YOUTUBE (Apr. 18, 2023), https://www.youtube.com/watch?v=1OQ5T9D9jbE&t=3; Sarah Perez, *FTC warns that AI technology like ChatGPT could 'turbocharge' fraud*, TECH CRUNCH (Apr. 18, 2023), https://techcrunch.com/2023/04/18/ftc-warns-congress-that-ai-technology-like-chatgpt-could-turbocharge-fraud-and-scams/ [https://perma.cc/82JP-JQDV].

72. Atleson, *supra* note 48.

73. Brewster, *supra* note 7.

74. Public Service Announcement, Fed. Bureau of Investigation, Deepfakes and Stolen Pill Utilized to Apply for Remote Work Positions (June 28, 2022), https://www.ic3.gov/Media/Y2022/PSA220628 [https://perma.cc/3NY5-ALJ6].

75. Joseph Cox, *GPT-4 Hired Unwitting TaskRabbit Worker By Pretending to Be 'Vision-Impaired' Human*, VICE (Mar. 15, 2023), https://www.vice.com/en/article/jg5ew4/gpt4-hired-unwitting-taskrabbit-woABer [https://perma.cc/P72S-FZDF].

76. Stuart A. Thompson, *Making Deepfakes Gets Cheaper and Easier Thanks to A.I.*, N.Y. TIMES (Mar. 12, 2023), https://www.nytimes.com/2023/03/12/technology/deepfakes-cheapfakes-videos-ai.html; Khoa Lam, *Incident 481: Deepfake TikTok Video Featured Joe Rogan Endorsing Supplement Brand*, AI INCIDENT DATABASE (Feb. 12, 2023), https://incidentdatabase.ai/cite/508.

images generated by Midjourney's AI tool to falsely portray the arrest of former President Donald Trump.[77] These images went viral after he claimed that his arrest was imminent.[78] In another alarming case, a fake AI-enabled video depicted President Joe Biden declaring a national draft in response to the Russian-Ukrainian war.[79]

In response to such concerning episodes, legislators at the federal and state levels have proposed bills to address deepfake technology and its potential impact on American elections. For instance, in June 2024, Senator Ted Cruz (R-TX) introduced a bipartisan bill, "Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks ("TAKE IT DOWN") Act," which aims to combat non-consensual deepfake pornography. The bill would criminalize the publication of such content without the victim's consent and require platforms to remove such imagery upon requests of the victim.[80] Rep. Yvette Clarke (D-NY) also introduced a bill[81] requiring disclosures on AI-generated content in political campaign ads. Rep. Ritchie Torres (D-NY) introduced a bill that requires a disclaimer on generative AI created content.[82] Several states have already passed laws pertaining to deepfake technology. In 2019, Texas[83] became the first state to criminalize political deepfake videos within thirty days of an election.

77. Isaac Stanley-Becker & Naomi Nix, *Fake images of Trump arrest show 'giant step' for AI's disruptive power*, Wash. Post (Mar. 22, 2023) https://www.washingtonpost.com/politics/2023/03/22/trump-arrest-deepfakes/ [https://perma.cc/E6W8-8HTU]; Kayleen Devlin & Joshua Cheetham, *Fake Trump arrest photos: How to spot an AI-generated image*, BBC (Mar. 24, 2023), https://www.bbc.com/news/world-us-canada-65069316 [https://perma.cc/3WQ8-6TF8].

78. Juliana Kim, *Trump claims that he will be arrested this week*, NPR (Mar. 19, 2023), https://www.npr.org/2023/03/18/1164524389/trump-claims-arrest-stormy-daniels [https://perma.cc/HV69-NDHB].

79. Thompson, *supra* note 76.

80. Press Release, Ted Cruz, Sen. Cruz Leads Colleagues In Unveiling Landmark Bill To Protect Victims Of Deepfake Revenge Porn (Jun. 18, 2024), https://www.cruz.senate.gov/newsroom/press-releases/sen-cruz-leads-colleagues-in-unveiling-landmark-bill-to-protect-victims-of-deepfake-revenge-porn [https://perma.cc/MHX4-D45E].

81. Press Release, Yvette D. Clarke, House of Representatives, Clarke Introduces Legislation to Regulate AI In Political Advertisements (May 2, 2023), https://claABe.house.gov/claABe-introduces-legislation-to-regulate-ai-in-political-advertisements/ [https://perma.cc/WK2Q-BJ5V].

82. Andrew Solender & Maria Curi, *Scoop: House Democrat's bill would mandate AI disclosure*, Axios (June 3, 2023), https://www.axios.com/2023/06/03/house-democrats-ritchie-torres-ai-disclosure.

83. Kenneth Artz, *Texas Outlaws 'Deepfakes'—but the Legal System May Not Be Able to Stop Them*, Law.com (Oct. 11, 2019), https://www.law.com/texaslawyer/2019/10/11/texas-outlaws-deepfakes-but-the-legal-system-may-not-be-able-to-stop-them/ [https://perma.cc/627W-J43R].

Shortly after, California[84] enacted a law prohibiting the production or distribution of "materially deceptive" videos about a candidate within 60 days of any election.[85] Illinois[86] recently passed bills to provide legal recourse for those who have been harmed by digital forgeries.

The music business is one of the industries most publicly contending with unauthorized AI content generation capabilities. Last year, a TikTok artist used AI-generated vocals[87] to imitate Drake and The Weeknd and then posted the alleged collaboration on social media. In response, James Murtagh-Hopkins, senior vice president of communications at UMG—the label that represents the two recording artists—stated, "[t]hese instances demonstrate why platforms have a fundamental legal and ethical responsibility to prevent the use of their services in ways that harm artists."[88] Eventually, both TikTok and YouTube pulled the track from their platforms; however, the question of how to address future AI-generated songs remains unclear. Grimes, another popular artist, announced this year that she would "split 50% royalties on any successful AI generated song that uses [her] voice."[89] This approach may not resonate with all artists, and some could instead turn to intellectual property or consumer protection law to challenge uses of their likeness.[90]

84. Amre Metwally, *Manipulated Media: Examining California's Deepfake Bill*, JOLT DIGEST (Nov. 12, 2019), https://jolt.law.harvard.edu/digest/manipulated-media-examining-californias-deepfake-bill [https://perma.cc/SYA5-8PV6].

85. This law expired in January 2023. Colin Lecker, *California has banned political deepfakes during election season*, THE VERGE (Oct. 7, 2019), https://www.theverge.com/2019/10/7/20902884/california-deepfake-political-ban-election-2020 [https://perma.cc/4BEV-W75G].

86. Patrick M. Keck, *Digital forgeries bills advance out of House, Senate committees*, THE STATE J.-REG. (Mar. 9, 2023), https://www.sj-r.com/story/news/politics/state/2023/03/09/bills-allowing-deepfake-victims-to-sue-pass-committee-votes/69968885007/ [https://perma.cc/D4K9-ETAS].

87. Nilay Patel, *AI Drake just set an impossible legal trap for Google*, THE VERGE (Apr. 19, 2023) https://www.theverge.com/2023/4/19/23689879/ai-drake-song-google-youtube-fair-use.

88. *Id*.

89. Mia Jankowicz, *Grimes offers a 50-50 split of royalties from successful AI-generated songs that use her voice*, BUS. INSIDER (Apr. 24, 2023), https://www.insider.com/grimes-offers-50-50-royalty-split-ai-songs-her-voice-2023-4 [https://perma.cc/KNY7-TANL].

90. Nikole Killion & Analisa Novak, *Music producers push for legal protections against AI: "There's really no regulation"*, CBS NEWS (Dec. 27, 2023), https://www.cbsnews.com/news/music-producers-lawmakers-artificial-intelligence/ [https://perma.cc/2S9W-MM2D].

C. Torts

Integration of AI into consumer-facing and clinical technologies, such as self-driving cars and medical devices, is likely to reshape liability landscapes.

Self-driving cars, or autonomous cars ("AC"), for instance, could reshape liability for road accidents. After an accident involving an AC, courts will need to decide who bears the responsibility—the owner of the car, the manufacturer, or the designer of the AI system. According to the 2023 Stanford AI Index, there was only one AI-related tort case in the U.S. in 2022 amidst 110 other AI-related legal cases, but given the increased use of AI in consumer products, this number is likely to grow significantly.[91]

Negligence standards could be applicable to products and devices that employ AI technology, including in data analytics services and medical devices. For instance, a product's design, the company's hiring practices, or management and overlay with AI systems all could present forms of negligence. Experts have identified four complications in applying traditional negligence laws to AI systems: unpredictability of AI errors, human limitations in interacting with AI, AI-specific software vulnerabilities in decision-making, and potential bias in AI.[92]

Product liability and strict liability frameworks present additional legal considerations for companies deploying AI technologies. For instance, when litigants identify flaws in product design or manufacture, or claim inadequate warnings of potential hazards, AI-related product liability law will likely expand[93] and assign responsibility in AI-related personal injury or property damage cases.

Currently, plaintiffs face several challenges when suing under traditional product liability frameworks.[94] In such a suit a plaintiff first would have to prove the defect was present before the AI left the developer or manufacturer's control, which is challenging since it

---

91. Nestor Maslej et al., The AI Index 2023 Annual Report, Stan. Inst. for Hum.-Centered A.I. (Apr. 2023), https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf [https://perma.cc/2HKS-5QCT].

92. Andrew D. Selbst, *Negligence and AI's Human Users*, 100 B.U. L. Rev. 1315, 1321–22 (2020).

93. John Villasenor, *Products liability law as a way to address AI harms*, Brookings (Oct. 31 2019) https://www.brookings.edu/research/products-liability-law-as-a-way-to-address-ai-harms/.

94. Priya Roy & Rituraj Bhowal, *An Analysis of Product Liability for AI Entities with special reference to the Consumer Protection Act, 2019*, 17 J. of Digit. Forensics, Sec. & L. (forthcoming at https://commons.erau.edu/jdfsl/vol17/iss2/3/); 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/HU33-7GHG].

may be hard to determine the root cause of the harm and when that impacted the pattern identified, and because AI systems evolve with new inputs and data.[95] Second, traditional upstream or downstream supply chain liability may be difficult to determine since liability could be negated if the retailer, at the time of controlling the product, was not able to determine whether a defect in the AI existed due to a lack of transparency and AI's adaptive qualities. Third, the plaintiff must show there was a reasonable alternative design (or "feasible alternative design") to the defective AI product, but there is no industry consensus on what would constitute such a "viable alternative."[96] For instance, there is no agreement on how to properly diversify the data used by an AI system in order to avoid biased outcomes.

Although some courts have declined to classify AI as a product,[97] there is reason to believe it could be classified as such once AI is incorporated into a device.[98] This distinction matters because "services" are only subject to negligence liability, while "products" are subject to both strict and negligence liability.[99] As AI use continues to expand in the medical field, courts could redefine "product" to include AI devices, thereby subjecting manufacturers to product liability claims. This appears imminent as use of AI in medical imaging and diagnostics is rapidly accelerating. The FDA cleared approximately ninety-one AI-enabled medical devices in 2022.[100] Additionally, a physician who uses an AI-enabled medical device for guidance that results in misdiagnosis or provides treatment inconsistent with established norms, protocols, or standards of care, could potentially face medical malpractice liability.[101]

Another area of tort concern for AI deployers is potential liability from a "failure to warn or instruct"—meaning if users claim they were not adequately informed about a product's limitations. While scholars

95. McNulty, *supra* note 94.

96. Frank J. Vandall, *Constructing a Roof Before the Foundation Is Prepared: The Restatement (Third) of Torts: Products Liability Section 2(b) Design Defec*t, 30 U. MICH. J. L. REFORM 261, 262 (1997).

97. Rodgers v. Christie, No. 19-2616, 2020 WL 1079233 (3d Cir. 2020).

98. Shook, Hardy & Bacon LLP, *Is Your Artificial Intelligence a Service or a Product?*, JD SUPRA, (Sept. 13, 2022), https://www.jdsupra.com/legalnews/is-your-artificial-intelligence-a-9959187/ [https://perma.cc/6VUU-5RC6].

99. Villasenor, *supra* note 93.

100. Joseph E. Fornadel, III, *Artificial Intelligence & Product Liability: Limitless Possibilities*, THE LIFE SCIS. LAB NELSON MILLER (Jan. 26, 2023), https://www.nelsonmullins.com/idea_exchange/blogs/the-life-sciences-lab/all/artificial-intelligence-and-product-liability-limitless-possibilities-the-life-sciences-lab [https://perma.cc/E5S9-VBJV].

101. William A. Tanenbaum et al., *Theories of AI liability: It's still about the human element*, REUTERS (Sept. 20, 2022), https://www.reuters.com/legal/litigation/theories-ai-liability-its-still-about-human-element-2022-09-20/.

have discussed the economics of the intersection of robotics and tort law,[102] and assessing AI defects based on overall system performance rather than individual product failures,[103] fewer articles have addressed the duty of care to provide warnings for defects when assessing AI products.[104] In *Hudson v. Tesla*, the defendant was alleged to have misled consumers about the safety and necessary human oversight of its autopilot program.[105] The complaint emphasized that Tesla "owed a duty of care to provide adequate warnings and instructions" regarding the autopilot system.[106] More recently, a class action lawsuit was filed against Tesla related to "phantom breaking" associated with its autopilot system.[107] The complaint alleged that Tesla fraudulently hid safety risks linked to its autopilot driver assist system, breaching its warranties and violating California's unfair competition law. In the event of a crash, such as the eight-car pile-up caused by a Tesla vehicle in "full self-driving" mode, a manufacturer could be deemed liable for tort liability.[108]

Some experts advocate for a new scheme of tort liability for AI, such as strict liability for instances of personal injury and death, and/or a fault-based liability structure for reputation and dignity harms.[109] Another proposal comes from the law commissions of England, Wales, and Scotland that focus on harms specifically caused by autonomous vehicles. The commissions published a joint report in

---

102. *See, e.g.*, Alessandro De Chiara et. al., *Car Accidents in the Age of Robots*, 68 INT'L REV. L. & ECON. 1 (2021).

103. Alice Guerra et. al., *Liability for robots II: An economic analysis*, 18 J. OF INSTITUTIONAL ECON. 553, 553–68 (2022); Eric Talley, *Automatorts: How should accident law adapt to autonomous vehicles? Lessons from law and economics* (Hoover Inst. Working Grp. on Intell. Prop., Innovation, & Prosperity at Stan. Univ., Working Paper No. 19002, 2019).

104. Ruth Janal, *Extra-Contractual Liability for Wrongs Committed by Autonomous Systems*, *in* ALGORITHMS AND LAW (Martin Ebers & Susana Navas eds., 2020); Mark Geistfeld, *A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation*, 105 CALIF. L. REV. 1611, 1611–94 (2017); Gerhard Wagner, *Robot Liability*, *in* LIABILITY FOR ARTIFICIAL INTELLIGENCE AND THE INTERNET OF THINGS (Sebastian Lohsse, Reiner Schulze, & Dirk Staudenmayer eds., 2019).

105. Complaint, Hudson v. Tesla Inc., 2018-CA-011812-O (Fla. Cir. Ct. 2018).

106. *Id.* at 9.

107. Andrew J. Hawkins, *Tesla slapped with class action lawsuit over phantom braking problem*, THE VERGE (Aug. 30, 2022), https://www.theverge.com/2022/8/30/23328836/tesla-phantom-braking-problem-class-action-lawsuit [https://perma.cc/C8EF-CH8V].

108. Matt McFarland, *Tesla 'full self-driving' triggered an eight-car crash, a driver tells police*, CNN (Dec. 21, 2022), https://www.cnn.com/2022/12/21/business/tesla-fsd-8-car-crash/index.html [https://perma.cc/WTQ6-W8DE].

109. Baris Soyer & Andrew Tettenborn, *Artificial intelligence and civil liability—do we need a new regime?*, 30 INT'L J. OF L. & INFO. TECH. 385 (2022).

2022 recommending that a new "legal actor" be established to bear responsibility for self-driving vehicles.[110] The paper recommends that this new legal actor, whether it is the vehicle manufacturer or software developer, serve as the first "point of contact" bearing responsibility for self-driving vehicles.

In September 2022, the European Commission proposed updates to liability laws,[111] including the Product Liability Directive (the "PLD") and AI Liability Directive (the "AILD").[112] In December 2023, EU policymakers reached a political agreement on the PLD.[113] that enable compensation when software impacts the safety of products like robots, drones, and smart-home systems. For companies based outside of the EU's jurisdiction, an injured party could seek compensation from the company's representative in the EU. The proposal also allows plaintiffs to sue for compensation if they are victims of harm or privacy breaches due to provider, developer, or user faults or omissions in AI technology, including discrimination in AI-based recruitment.

Due to the technically complex nature of AI systems, the EU's proposal simplifies the victim's burden of proof by introducing a "presumption of causality."[114] The victim must demonstrate that a breach of certain requirements led to harm, and make the connection to the AI technology. There is also a provision for a "right of access to evidence" clause, which would enable victims to compel companies and suppliers to disclose information about high-risk AI systems to

110. L. COMM'N OF ENG. & WALES, AUTOMATED VEHICLES: JOINT REPORT (Jan. 25, 2022), https://cloud-platform-e218f50a4812967ba1215eaecede923f.s3.amazonaws.com/uploads/sites/30/2022/01/Automated-vehicles-joint-report-cvr-03-02-22.pdf [https://perma.cc/ZE2H-YK9S].

111. Press Release, Eur. Comm'n, New liability rules on products and AI to protect consumers and foster innovation (Sept. 28, 2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5807 [https://perma.cc/TRR7-R6LU].

112. *Commission Proposal for an Artificial Intelligence Liability Directive*, COM (2022) 496 final (Sept. 9, 2023) [hereinafter *Commission Proposal*], https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496.

113. Luca Bertuzzi, *EU updates product liability regime to include software, Artificial Intelligence*, EURACTIV (Dec. 14, 2023), https://www.euractiv.com/section/digital/news/eu-updates-product-liability-regime-to-include-software-artificial-intelligence/ [https://perma.cc/PBL4-A9AJ]; Julia Launders, *Beyond the AI Act: The AI Liability Directive & the Product Liability Directive*, A&L GOODBODY LLP (Mar. 5, 2024), https://www.techlaw.ie/2024/03/articles/artificial-intelligence/beyond-the-ai-act-how-the-ai-liability-directive-and-the-product-liability-directive-will-also-shape-the-regulation-of-ai-in-the-eu/ [https://perma.cc/DT6B-9RH9].

114. *Commission Proposal*, *supra* note 112; Kristina Elhe & Stephen Kreb, *AI Trends For 2023 - Increasing Product Liability For AI And Software In The EU*, JD SUPRA (Dec. 12, 2022), https://www.jdsupra.com/legalnews/ai-trends-for-2023-increasing-product-1515288/ [https://perma.cc/2XKR-UEHC].

determine the problem's source.[115] The European Economic and Social Committee recommends reviewing the AI Liability Directive around 2026.[116]

As regulations on product liability expand and evolve across the globe, businesses may choose to notify consumers and those in the supply chain that AI systems must operate with direct human oversight and evaluation. Scholars argue that companies benefiting from AI must also accept potential liability for harm caused by algorithms they have designed, including post-sale alterations that lead to unintended results.[117] They further contend that companies should not get away with a "blame the data" argument, and that users cannot be held accountable for using an AI system in a reasonably foreseeable way. Plaintiffs could argue instead for a vicarious liability scheme, which would hold an AI programmer liable for an AI's output.[118]

D. Expansion of Consumer Protection Regulatory Mechanisms for AI

In recent years, the FTC, the Securities Exchange Commission ("SEC"), and advocacy groups have considered various novel ways to regulate AI. As discussed above, the FTC has been clear on its intent to regulate in the AI space: "Hold yourself accountable—or be ready for the [regulatory agencies] to do it for you."[119] The FTC's authority to address AI threats to consumers derives from two sources: its investigation and reporting power under Section 6[120] of the FTC Act

115. In addition, the draft PLD outlines factors to determine the product's defectiveness, such as how the product is presented, adherence to product safety standards, the end user's specific expectations, and controls in the manufacturing process. *See* Michal Matejka & Eva Fialova, *New Rules on AI and Product Liability*, LEXOLOGY (Jan. 11, 2023), https://www.lexology.com/library/detail.aspx?g=75e60b8e-1839-4b73-83e8-2224e144df65 [https://perma.cc/WJ7P-W6L4]. The current revision contains AI, software, and Internet of Things digital services as "products" subject to strict product liability, and it includes certain fulfillment service providers and online marketplaces as parties subject to liability. For definition of Internet of Things, *see What is the Internet of Things (IoT)?*, IBM, https://www.ibm.com/topics/internet-of-things [https://perma.cc/C3LY-NZ6K]. Elhe & Kreb, *supra* note 114. The revision removes the liability cap on potential damages. *Id.*

116. Opinion of the European Economic and Social Committee on "Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)," 2023 O.J. (C 140) 5.

117. Villasenor, *supra* note 93.

118. McNulty, *supra* note 94.

119. Jillson, *supra* note 43.

120. Federal Trade Commission Act, 15 U.S.C. §§ 41–58.

and its rulemaking authority under Section 18.[121] Additionally, the SEC Investment Advisory Committee ("IAC") is exploring the SEC's authority to establish a framework for preventing harm to consumers by AI-powered investment advisory tools.[122]

1. Federal Trade Commission

Section 6 of the FTC Act empowers the agency to conduct investigations of persons, partnerships, or corporations that affect commerce and to require the submission of reports on the same. In March 2023, the Center for AI and Digital Policy filed a complaint calling for the FTC to use its Section 6 power to investigate OpenAI and "prevent the release of further models until necessary guardrails are established."[123] By requiring companies to submit reports, which can cover topics such as a company's "organization, business, conduct, practices, management, and relation to other corporations, partnerships, and individuals,"[124] Commissioner Slaughter highlighted that the FTC can "study in depth how algorithms and related technologies are being deployed and how [it] can effectively adapt to combat their harms."[125]

Another FTC regulatory tool is its authority to engage in Section 18 rulemaking.[126] Empowered by the Magnuson Moss Warranty-Federal Trade Commission Improvements Act,[127] the FTC may promulgate binding regulations that clarify legal limits, providing guidance to prevent future harms rather than waiting for enforcement actions to correct violations that have already occurred.[128] For example, the FTC utilized Section 18 authority in August 2022 to initiate creation of rules

121. 15 U.S.C. §§ 57(a).

122. Letter from Christopher Mirabile et al., Chair, Inv. Advisor Comm., to Hon. Gary Gensler, Chair, U.S. Sec. & Exch. Comm'n (Apr. 6, 2023), https://www.sec.gov/files/20230406-iac-letter-ethical-ai.pdf [https://perma.cc/XB8K-ZEJW] (proposing an ethical AI framework for investment advisors).

123. *In The Matter Of OpenAI*, Ctr. for AI & Digit. Pol'y, https://www.caidp.org/cases/openai/ [https://perma.cc/VB25-QE9Q] (last visited June 8, 2024); *see* Ctr. for AI & Digit. Pol'y, Complaint and Request for Investigation of OpenAI, L.P., to the Fed. Trade Comm'n (Mar. 30, 2023), https://www.caidp.org/app/download/8450269463/CAIDP-FTC-Complaint-OpenAI-GPT-033023.pdf.

124. 15 U.S.C § 46(b); Oren Bar-Gill et. al, *Algorithmic Harm in Consumer Markets,* J. of Legal Analysis (Aug. 21, 2023), https://academic.oup.com/jla/article/15/1/1/7246686.

125. Slaughter, *supra* note 43.

126. 16 C.F.R. § 1.18 (2021).

127. 15 U.S.C. §§ 2301–12.

128. Slaughter, *supra* note 43.

addressing automated decisions.[129] This process, referred to as the Commercial Surveillance and Data Security Rulemaking, sought public input on several topics, including automated systems, discrimination, consumer consent, notice, transparency, and disclosure.[130] Companies should note that the Commission may continue to shape AI use and regulation through this Section 18 rulemaking process.

2. Securities and Exchange Commission

The SEC has also sought to expand its authority to regulate in this area. As noted above, the SEC's IAC is investigating how AI, and in particular robo-advisers, will affect the financial sector. In March 2022, the SEC convened a "Panel Discussion Regarding Ethical AI and RoboAdvisor Fiduciary Responsibilities,"[131] which covered the benefits and risks of AI-powered advice and considered potential biases and blind spots of this technology.[132]

The SEC has made other indications of efforts to strengthen its oversight of AI used by financial firms. On April 6, 2023, the IAC wrote a letter to SEC Chair Gary Gensler regarding the establishment an ethical AI framework for investment advisors.[133] In urging the SEC to expand its guidance, the IAC advocated a focus on the following tenets when developing a regulatory framework: equity, consistent and persistent testing, and governance and oversight.

129. Fed. Trade Comm'n, *Commercial Surveillance and Data Security Rulemaking* (Aug. 11, 2022), https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking [https://perma.cc/S8T7-SUKC].

130. *Id.*

131. Inv. Advisory Comm., *Meeting Agenda*, U.S. Sec. & Exch. Comm'n (Mar. 1, 2022), https://www.sec.gov/spotlight/investor-advisory-committee/iac031022-agenda.htm [https://perma.cc/A7DT-SB7W].

132. EqualAI President and CEO Miriam Vogel testified before the IAC, addressing the need to identify and mitigate bias and harms that AI can present in the financial sector. U.S. Sec. & Exch. Comm'n, *03 10 2022 IAC Meeting Part 1*, YouTube (Mar. 11, 2022), https://www.youtube.com/watch?v=LFRahZVxVSQ.

133. Mirabile et al., *supra* note 122. The letter underscores the SEC's "ample authority" to monitor technology deployed in the investment advisory industry and calls on the commission to issue clear guidelines for SEC-regulated businesses. The letter adds that the SEC should consider the following characteristics identified by NIST in the AI Risk Management Framework (AI RMF): accuracy, interpretability, privacy, reliability, robustness, safety, resilience, and mitigation of harmful bias. AI RMF 1.0, *supra* note 17. The letter also notes that investment advisor clients already suffer from poor quality AI.

The SEC's track record of enforcement actions, such as those against Wealthfront Advisors,[134] Hedgeable,[135] Wahed Invest,[136] Schwab Subsidiaries,[137] and others, demonstrates its intent to hold robo-advisers accountable for illegal AI use. For example, in the Schwab case, the SEC charged three subsidiaries with misleading practices concerning robo-adviser portfolios, which resulted in a $187 million settlement to compensate clients. The SEC also has used its authority under Section 206 of the Investment Advisers Act[138] to fine firms for "AI washing," where there are false or misleading claims of AI use in investment strategies.[139] The SEC brought two enforcement actions, against Global Predictions, Inc., and Delphia, in March 2024, which resulted in settlements of $175,000 and $225,000, respectively.[140]

In July 2023, the SEC proposed new rules for broker-dealers and investment advisors (collectively, "firms").[141] Among other requirements, these rules would require firms using algorithms and other covered technologies to neutralize or eliminate conflicts of interest and to keep appropriate records.

II. Criminal Justice and Civil Rights Considerations

The following subsections explore the intersection of AI with the criminal justice system and due process protections, as well as U.S. civil rights law—including housing, hiring, disability, credit, and workers' rights.

---

134. Press Release, Sec. & Exch. Comm'n, SEC Charges Two Robo-Advisers With False Disclosures (Dec. 21, 2018), https://www.sec.gov/news/press-release/2018-300 [https://perma.cc/FG83-34FJ].

135. *Id.*

136. Press Release, Sec. & Exch. Comm'n, SEC Charges Robo-Adviser with Misleading Clients (Feb. 10, 2022), https://www.sec.gov/news/press-release/2022-24 [https://perma.cc/CLM9-9ZZC].

137. Press Release, Sec. & Exch. Comm'n, Schwab Subsidiaries Misled Robo-Adviser Clients about Absence of Hidden Fees (June 13, 2022) https://www.sec.gov/news/press-release/2022-104 [https://perma.cc/978V-WFYM].

138. 15 U.S. Code § 80b–6.

139. Jason Wallace, *'AI washing' meets marketing rule, as SEC fines two advisers for their AI claims*, Thomson Reuters (Mar. 26, 2024), (https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/ai-washing-enforcement/ [https://perma.cc/6Q8B-KAKN]; Sec. & Exch. Comm'n, *supra* note 134.

140. Sec. & Exch. Comm'n, *supra* note 134.

141. Press Release, Sec. & Exch. Comm'n, SEC Proposes New Requirements to Address Risks to Investors From Conflicts of Interest Associated With the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers (July 26, 2023), https://www.sec.gov/news/press-release/2023-140 [https://perma.cc/T6EL-W7XX].

A. Criminal Justice

AI use in law enforcement operations and surveillance, by both public and private actors, has been the focus of increased public attention. This has prompted one of the few areas of significant legislative activity at federal, state, and local levels resulting in new laws and the discontinuation, at least temporarily, of high-profile policing initiatives, as addressed in this section below.

The advent of surveillance technologies, including wiretapping,[142] heat sensors,[143] GPS tracking devices,[144] and cell-site location tracking,[145] has required courts and policymakers to continually revisit the limits of lawful government surveillance. AI-powered facial recognition technology ("FRT") software emerged in the past decade as a key surveillance tool for law enforcement[146] and national security agencies.[147] Under traditional Fourth Amendment jurisprudence, facial recognition technology used in public spaces does not contravene constitutional protections.[148] Accordingly, there is not currently reason to expect constitutional challenges to law enforcement's use of this technology. However, given the high impact of these uses on individuals and rights, there has been significant activity in legislatures and courtrooms to define its acceptable use cases and its limits. As such, awareness of how these uses of AI can create potential liability is important for any organization, and their counsel, who is using or considering use of such technologies.

There are several critical legal considerations that should guide any discussion of the use of AI surveillance tools. In a 2016 report, Georgetown Law's Center on Privacy & Technology found that one in two American adults are registered in a police facial recognition system. Numerous studies outline a history of disproportionate use

142. Olmstead v. United States, 277 U.S. 438 (1928).
143. Kyllo v. United States, 533 U.S. 27 (2001).
144. United States v. Jones, 565 U.S. 400 (2012).
145. Carpenter v. United States, 585 U.S. 262 (2018).
146. Nicol Turner Lee & Caitlin Chin-Rothmann, *Police surveillance and facial recognition: Why data privacy is imperative for communities of color*, Brookings (Apr. 12, 2022), https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ [https://perma.cc/RT5E-74LZ].
147. Rebecca Santana & Rick Gentilo, *TSA is testing facial recognition at more airports, raising privacy concerns*, AP News (May 15, 2023), https://apnews.com/article/facial-recognition-airport-screening-tsa-d8b6397c02afe16602c8d34409d1451f [https://perma.cc/R4HH-UHVS].
148. Andrew Ferguson, *Facial Recognition and the Fourth Amendment*, 105 Minn. L. Rev. 1105, 1128 (2021), https://digitalcommons.wcl.american.edu/facsch_lawrev/742 [https://perma.cc/82GE-2BPC].

of surveillance technology on communities of color in the United States.[149] As a result, when AI systems are trained on these biased datasets that over-index on surveillance of certain communities, the AI system will reproduce and reinforce these patterns when making recommendations.[150] Additionally, numerous studies have shown that FRT has historically demonstrated biases[151] and disproportionate inaccuracy in recognizing or "seeing" people of color.[152] A 2019 study found that "[f]or one-to-one matching, *most systems had a higher rate of false positive matches for Asian and African American faces over Caucasian faces, sometimes by a factor of 10 or even 100*."[153]

Public awareness of these inaccuracies led to the emergence of legislation and corporate action to pause or limit law enforcement's use of the technology. For instance, the Facial Recognition Act of 2022, introduced by Representatives Ted Lieu (CA-36), Sheila Jackson Lee (TX-18), Yvette Clarke (NY-9), and Jimmy Gomez (CA-34), aimed "to place strong limits and prohibitions on law enforcement use of facial recognition technology."[154] Among other provisions, the bill requires law enforcement agencies to obtain a court order to use FRT, except in specific emergency situations; requires agencies using facial recognition to log their usage and undergo regular audits; and requires

149. Lee & Chin-Rothmann, *supra* note 146.

150. Molly Callahan, *Algorithms Were Supposed to Reduce Bias in Criminal Justice—Do They?*, THE BRINK (Feb. 23, 2023), https://www.bu.edu/articles/2023/do-algorithms-reduce-bias-in-criminal-justice/ [https://perma.cc/3H4W-ZPNA]; Nicol Turner Lee et al., *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms*, BROOKINGS (May 22, 2019), https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/ [https://perma.cc/DE2L-DGZT]; Julia Angwin, *Machine Bias*, PRO PUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/NUV8-3SMF].

151. Alex Najibi, *Racial Discrimination in Face Recognition Technology*, SCI. IN THE NEWS (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/ [https://perma.cc/Q7XU-D78M].

152. Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. OF MACH. LEARNING RSCH. 1 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf [https://perma.cc/JXM2-M6P3].

153. Karen Hao, *A U.S. government study confirms most face recognition systems are racist*, MIT TECH. REV. (Dec. 20, 2019), https://www.technologyreview.com/2019/12/20/79/ai-face-recognition-racist-us-government-nist-study/ [https://perma.cc/8YTZ-GKMN?type=image] (emphasis added).

154. Press Release, Ted Lieu, Rep., H.R., Reps Ted Lieu, Sheila Jackson Lee, Yvette Clarke, and Jimmy Gomez Introduce Bill to Regulate Law Enforcement Use of Facial Recognition Technology (Sept. 29, 2022), https://lieu.house.gov/media-center/press-releases/reps-ted-lieu-sheila-jackson-lee-yvette-clarke-and-jimmy-gomez-introduce [https://perma.cc/U89L-LU86].

these agencies to report their activities to oversight bodies and make these reports available to the public.[155]

Concerns about citizens' privacy and false identification also led state legislatures in Maine,[156] Virginia,[157] and Massachusetts,[158] as well as numerous municipalities,[159] including San Francisco[160] and New Orleans,[161] to restrict or even ban the use of FRT by law enforcement. Many of these FRT laws also create a private right of action against law enforcement agencies by individuals who believe they were unfairly targeted

Among the most prominent examples of a FRT law that resulted in significant legal liability is Illinois' Biometric Information Privacy Act ("BIPA").[162] In a landmark case, the ACLU alleged that Clearview AI violated BIPA by collecting facial recognition data without the consent of the subjects whose data Clearview had collected.[163] Clearview AI ultimately agreed to a settlement that included a permanent injunction preventing the sale or distribution of face photographs within its

155. H.R. Res. 9061, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/house-bill/9061/text?s=1&r=7 [https://perma.cc/MN36-TLBW].

156. Grace Woodruff, *Maine Now Has the Toughest Facial Recognition Restrictions in the U.S.*, SLATE (July 2, 2021), https://slate.com/technology/2021/07/maine-facial-recognition-government-use-law.html [https://perma.cc/5G6C-ARRP].

157. Va. Code Ann. §§ 15.2–1723.2, 23.1–815.1 (2021) https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+HB2031ER+hil [https://perma.cc/ZA94-2CAE].

158. Will Katcher, *Massachusetts Commission Sets Facial Recognition Guidelines*, GOVERNING (Mar. 22, 2022), https://www.governing.com/security/massachusetts-commission-sets-facial-recognition-guidelines [https://perma.cc/5MLC-BAY7].

159. *Ban Facial Recognition*, FIGHT FOR THE FUTURE, https://www.banfacialrecognition.com/map/ [https://perma.cc/J3SD-T4XD] (last visited May 24, 2024).

160. Dave Maas, *San Francisco Police Nailed for Violating Public Records Laws Regarding Face Recognition and Fusion Center Documents*, ELEC. FRONTIER FOUND. (June 2, 2022), https://www.eff.org/deeplinks/2022/06/san-francisco-police-nailed-violating-public-records-laws-regarding-face#:~:text=In%20the%20summer%20of%202019,in%20order%20to%20establish%20identity [https://perma.cc/6CZQ-JZWS].

161. Michael Isaac Stein, *New Orleans police use of facial recognition nets zero arrests in nine months*, LOUISIANA ILLUMINATOR (July 28, 2023), https://lailluminator.com/2023/07/28/new-orleans-police-use-of-facial-recognition-nets-zero-arrests-in-9-months/ [https://perma.cc/B577-4EKK]; New Orleans ultimately lifted the ban on surveillance technology; however, in the thirteen times it was used between October 1, 2022, and July 1, 2023, zero arrests were made. *Id.*

162. Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14 (2024) https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57 [https://perma.cc/9ESF-5VCJ].

163. *ACLU v. Clearview AI*, ACLU (May 11, 2022), https://www.aclu.org/cases/aclu-v-clearview-ai [https://perma.cc/X7PA-ZPXM].

database.[164] This legal action followed another case addressing privacy concerns surrounding FRT. As a result of a class action lawsuit on behalf of 1.6 million users against Facebook based on its opt-in regime of automatically tagging members in photos, Facebook agreed to pay $650 million.[165]

Given the increased number of and success of such legal actions,[166] companies such as Meta curbed their FRT use[167] while others, including Microsoft[168] and Amazon,[169] agreed not to sell this technology to law enforcement for a certain period of time.[170]

However, the gradual improvement of AI accuracy, coupled with rising crime rates in certain areas of the country, prompted some cities to reconsider these limits and bans.[171] For instance, Clearview AI saw a 26 percent increase in law enforcement use of its FRT the day after the January 6 attack at the Capitol.[172]

---

164. Adi Robertson, *Clearview AI agrees to permanent ban on selling facial recognition to private companies*, THE VERGE (May 9, 2022), https://www.theverge.com/2022/5/9/23063952/clearview-ai-aclu-settlement-illinois-bipa-injunction-private-companies [https://perma.cc/WC23-RTB9].

165. Kim Lyons, *Judge approves $650 million Facebook privacy settlement over facial recognition feature*, THE VERGE (Feb. 27, 2021), https://www.theverge.com/2021/2/27/22304618/judge-approves-facebook-privacy-settlement-illinois-facial-recognition [https://perma.cc/SW8U-FV4E].

166. Andrew Blancher, *An Analysis of Facial Recognition Technology Lawsuits*, VERISK (Nov. 30, 2022), https://www.verisk.com/insurance/visualize/an-analysis-of-facial-recognition-technology-lawsuits/ [https://perma.cc/SWH5-M8EW].

167. Jerome Pesenti, *An Update On Our Use of Face Recognition*, META (Nov. 2, 2021), https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/ [https://perma.cc/X5ZY-NGCH].

168. Jay Greene, *Microsoft won't sell police its facial recognition technology following similar moves by Amazon and IBM*, WASH. POST (June 11, 2020). https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/ [https://perma.cc/NN9S-WQFN].

169. David Jeans, *Amazon Extends Moratorium On Police Use Of Facial Recognition Technology*, FORBES (May 18, 2021), https://www.forbes.com/sites/davidjeans/2021/05/18/amazon-indefinitely-bans-police-use-of-facial-recognition-technology/?sh=28a26c15401b [https://perma.cc/JYY2-TUTE].

170. However, it is unclear if these moratoria remain. For instance, the Department of Justice has revealed that the FBI may be beginning to use Amazon Rekognition, a controversial image and video analysis software known for its facial recognition capabilities, as indicated in an update to the agency's AI technology inventory. Rebecca Heilweil & Madison Alder, *Justice Department discloses FBI project with Amazon Rekognition tool*, FEDSCOOP (Jan. 25, 2024), https://fedscoop.com/doj-fbi-amazon-rekognition-technology-ai-use-case/ [https://perma.cc/NQ69-WAGR].

171. Paresh Dave, *Focus: U.S. cities are backing off banning facial recognition as crime rises*, REUTERS (May 12, 2022), https://www.reuters.com/world/us/us-cities-are-backing-off-banning-facial-recognition-crime-rises-2022-05-12/ [https://perma.cc/W3PP-VVBW].

172. Kim Lyons, *Use of Clearview AI facial recognition tech spiked as law enforcement seeks to identify Capitol mob*, THE VERGE (Jan. 10, 2021), https://www.

There are also use cases of AI that are less controversial, such as use by law enforcement to combat human trafficking. The Global Emancipation Network and Thorn, in partnership with Microsoft, have utilized AI technologies to better detect, and therefore more quickly rescue, victims of sex and child trafficking by analyzing online ads and platforms for signs of exploitation.[173]

Generative AI has further altered the law enforcement landscape. In the U.S., 69 percent of exonerations by DNA evidence have involved mistaken identification.[174] As part of a hackathon in 2022, developers created a program that harnessed DALL-E 2, an AI program developed by OpenAI that generates images from textual descriptions, to create "hyper-realistic" AI-generated police sketches by using human descriptions of facial features.[175] However, such a program may scale and distort human biases through its design instead of fixing them.[176] Research suggests that humans remember faces holistically rather than by individual features,[177] meaning that once the AI-generated image has been created, it becomes ingrained into the witness's memory. These highly realistic AI-generated sketches could lead witnesses and the public to falsely accuse innocent people, thereby exacerbating societal biases and causing, rather than reducing, misidentifications.[178]

Facial recognition technology is just one type of AI that is used in law enforcement and the criminal justice system. Predictive policing—used to forecast criminal activity—is another way police departments have incorporated AI into law enforcement practices.[179] However, AI

---

theverge.com/2021/1/10/22223349/clearview-ai-facial-recognition-law-enforcement-capitol-rioters [https://perma.cc/LX9P-KK4Z].

173. *Combating Human Trafficking: How Ai Revolutionizes The Fight*, Veritone, https://www.veritone.com/blog/ai-public-safety-human-trafficking/ [https://perma.cc/4R58-EDXK].

174. *How Eyewitness Misidentification Can Send Innocent People to Prison*, Innocence Project (Apr. 15, 2020), https://innocenceproject.org/news/how-eyewitness-misidentification-can-send-innocent-people-to-prison/ [https://perma.cc/SK5S-HUKJ].

175. Chloe Xiang, *Developers Created AI to Generate Police Sketches. Experts Are Horrified*, Vice (Feb. 7, 2023), https://www.vice.com/en/article/qjk745/ai-police-sketches?utm_source=substack&utm_medium=email [https://perma.cc/8UGR-WN4M].

176. Clare Garvie, Ctr. on Priv. & Tech. at Geo. L., A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations 31 (Dec. 6, 2022), https://www.law.georgetown.edu/privacy-technology-center/publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations/ [https://perma.cc/7XGN-P5B5].

177. Xiang, *supra* note 175.

178. *Id.*

179. Tim Lau, *Predictive Policing Explained*, Brennan Ctr. for Just. (Apr. 1, 2020), https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained [https://perma.cc/S3T2-UVQ6].

systems used for predictive policing are often skewed. For instance, training data could be based on data that was released under a consent decree, which means it was collected based on past findings of a police unit's discriminatory practices. As a result, using such an AI tool, trained on biased or "dirty" data, may present a serious risk of perpetuating further bias and discriminatory practices.[180] Tools such as PredPol are trained on prior policing data, which may cause a reinforcing feedback loop: if a certain community is disproportionately policed due to human bias, the tool will recommend police deployment to that community without an adequate basis for such a recommendation.[181] In short, a tool is only helpful if trained on data where past practice is based on meaningful determinations, but not if it is based on biased or arbitrary decisions and activity.

Predictive policing also could raise constitutional questions around the reasonable suspicion doctrine.[182] Predictive policing involves algorithms that analyze patterns and trends. The insights generated by these algorithms are used to make predictions about issues such as where crimes are likely to occur, who might be involved, and when they might happen.[183] Under the Fourth Amendment, law enforcement must have probable cause to conduct a search, or a reasonable suspicion to stop or seize.[184] To justify reasonable suspicion, police must "be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion."[185] Although the Supreme Court considered other predictive indicators that weigh into reasonable suspicion and determined they were acceptable—such as tips, profiles, and high crime areas—it has not yet decided how predictive policing tools should factor into the reasonable suspicion analysis.[186]

180. Rasguda Richardson et al., *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. Rev. Online 192 (2019), *available at* https://www.nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson_etal-FIN.pdf [https://perma.cc/QV46-KZQX].

181. Jacob Metcalf, *Ethics review for pernicious feedback loops*, Medium (Nov. 7, 2016), https://medium.com/datasociety-points/ethics-review-for-pernicious-feedback-loops-9a7ede4b610e [https://perma.cc/XTJ2-SLRR].

182. Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion* 62 Emory L. J. 259, 263 (2012), https://digitalcommons.wcl.american.edu/facsch_lawrev/750/ [https://perma.cc/C3TT-XWBQ].

183. Tzu-Wei Hung & Chun-Ping Yen, *Predictive policing and algorithmic fairness*, 201 Synthese at *4 (2023), https://doi.org/10.1007/s11229-023-04189-0 [https://perma.cc/EYH7-W4V6].

184. U.S. Const. amend. IV.

185. Terry v. Ohio, 392 U.S. 1, 21 (1968).

186. Ferguson, *supra* note 182, at 263.

The Los Angeles, New York, and Chicago police departments have all used versions of predictive policing in recent years.[187] The LAPD, for instance, used a tool called LASER (Los Angeles Strategic Extraction and Restoration) to predict gun violence, along with PredPol to predict areas of property-related crimes.[188] However, after an audit found inconsistencies in the LASER program's selection and retention processes, LAPD discontinued use of the program.[189] In 2020, the LAPD stated it would cease using PredPol due to financial constraints.[190]

Additionally, algorithmic tools for risk assessment ("RAI") have been used by judges to decide whether to grant bail, make sentencing recommendations and determinations, and dictate probation and parole requirements.[191] Critics of these algorithms have raised concerns ranging from their lack of individualization in making recommendations and an absence of transparency to the incidence of bias.[192] In Flores v. Stanford, a non-party to the case, Northpointe, Inc., sought to prevent the disclosure of proprietary information related to their COMPAS tool after it was requested by the plaintiff. The New York court denied Northpointe's request and emphasized that the materials were relevant to the plaintiffs' constitutional claims and that the plaintiffs deserved the chance to look into the workings of the AI system when decisions are made about them.[193]

In *Flores,* plaintiffs were denied parole and sued the New York State Board of Parole based on its use of correctional offender management profiling for alternative sanctions ("COMPAS"). Northpointe, Inc., the creator of COMPAS, petitioned the court seeking to block the disclosure of information about its AI system, arguing that the information was a protected trade secret.[194] The court, however, determined that the information was relevant to the case and could be disclosed under a

187. Lau, *supra* note 179.
188. *Id.*
189. *Id.*
190. Leila Miller, *LAPD will end controversial program that aimed to predict where crimes would occur*, L.A. TIMES (Apr. 21, 2020), https://www.latimes.com/california/story/2020-04-21/lapd-ends-predictive-policing-program.
191. Alex Chohlas-Wood, *Understanding risk assessment instruments in criminal justice*, BROOKINGS (June 19, 2020), https://www.brookings.edu/research/understanding-risk-assessment-instruments-in-criminal-justice/ [https://perma.cc/T7RH-LKEH]; Sarah Valentine, *Impoverished Algorithms: Misguided Governments, Flawed Technologies, and Social Contro*l, 46 FORDHAM URB. L.J. 364, 411 (2019), https://ir.lawnet.fordham.edu/ulj/vol46/iss2/4 [https://perma.cc/75CA-4MCX].
192. Chohlas-Wood, *supra* note 191.
193. Flores v. Stanford, 18 Civ. 02468 (VB)(JCM) (S.D.N.Y. Sept. 28, 2021) https://casetext.com/case/flores-v-stanford-2 [https://perma.cc/V7WM-QKF3].
194. *See* MASLEJ ET AL., *supra* note 91, at 295 (summarizing *Flores*).

protective order.[195]As this case demonstrates, even when an algorithm is used to make a decision, those who are affected are still entitled to know how the decision was made. This should stand as a signal to companies developing RAI and other tools that their proprietary rights will not outweigh the protections afforded in the justice system.

B. Benefits Determinations

In addition to law enforcement and the judicial system, government agencies that offer benefits have increased adoption of AI systems to improve decision-making processes in numerous areas related to social policy.[196] Algorithms have been used for benefits administration, such as Medicaid determinations; termination from public employment; and other welfare allocations. However, government use of AI can raise procedural due process issues. Because these benefits are treated as property rights, they are subject to constitutional and statutory protections, such as the right to notice, an opportunity to be heard, a determination made by a neutral decision-maker, and a requirement that the government explain why and how it decided to take action to reduce or terminate benefits.[197]

In the canonical *Mathews v. Eldridge* case, the Supreme Court established a three-factor framework for determining whether the government had satisfied constitutional due process requirements when making benefits determinations: "(1) the private interest, (2) the risk of erroneous deprivation, and (3) the governmental interest (especially fiscal and administrative)."[198] The use of privately developed algorithms to provide public benefits determinations has spurred numerous disputes, including those addressed in *Michael T. v. Crouch.*[199]

Crouch,[200] litigated in 2018, demonstrates how an algorithm's lack of transparency can violate individuals' due process rights in the

195. *Flores*, 18 Civ. 02468, at 11.

196. Danielle Keats Citron, *Technological Due Process*, 85 Wash. U. L. Rev. 1249, 1252 (2008), https://openscholarship.wustl.edu/law_lawreview/vol85/iss6/2 [https://perma.cc/LX84-42BX]; Valentine, *supra* note 191, at 365; Bloch-Wehba, *supra* note 5, at 1266–67; Christine Chambers Goodman, *AI, Can You Hear Me? Promoting Procedural Due Process in Government Use of Artificial Intelligence Technologies*, 28 Rich. J.L. & Tech. 700, 700 (2022), https://jolt.richmond.edu/vol-xxviii-issue-4/ [https://perma.cc/GQ6J-K26C].

197. Bloch-Wehba, *supra* note 5, at 1275.

198. Goodman, *supra* note 196 (citing Mathews v. Eldridge, 424 U.S. 319, 348–49 (1976)).

199. No. 2:15-CV-09655, 2018 WL 1513295, at *2 (S.D. W. Va. 2018).

200. Michael T. v. Crouch, No. 2:15-CV-09655, 2018 WL 1513295, at *2 (S.D. W. Va. 2018).

Medicaid arena.[201] In the case, a group of plaintiffs challenged West Virginia's proprietary algorithm that reduced their Medicaid benefits. One plaintiff's Medicaid benefits had been cut nearly in half, requiring her to leave her home and move to an emergency care facility. The benefits determination had been made by a private company's algorithmically-driven tool used to conduct annual assessments of Medicaid recipients' needs. The court found that the government's use of this algorithm failed to meet the Constitution's due process requirements as it did not provide plaintiff information on the standards used in the algorithm and failed to employ an individualized assessment for the allocation to plaintiffs, denying plaintiffs the opportunity to challenge the benefits determination.[202]

C. Civil Rights

The DOJ and EEOC have also joined the federal agencies in announcing their active monitoring of automated systems that "may contribute to discrimination and otherwise violate federal law."[203] AI systems can reflect and exacerbate biases related to gender, race,[204] and age, among other protected categories, based on patterns it learns the data the systems were trained on (for example, redlining in mortgage lending data), the questions the algorithms are trained to answer (for example, determining appropriate care to offer patients based on past costs rather than past health outcomes), and the parameters of their models.[205] Without appropriate supervision and interrogation, uses of AI can unfairly disadvantage or discriminate, denying civil rights, benefits, or appropriate care. This section explores how current civil rights laws may be applicable to AI systems.

Civil rights laws safeguard protected classes[206] under decades of established precedent, and federal agencies with oversight and authority

201. Bloch-Wehba, *supra* note 5, at 1291 n.199.

202. *Id.* at 1278 (citing Michael T. v. Bowling, No. 2:15-CV-09655, 2016 WL 4870284, at *10 (S.D.W. Va. Sept. 13, 2016), *modified sub nom.* Michael T. v. Crouch, 2018 WL 1513295 (S.D.W. Va. Mar. 26, 2018).

203. Chopra, *supra* note 41.

204. Pranshu Verma, *These Robots were trained on AI. They Became Racist and Sexist*, Wash. Post (July 16, 2022 6:00 AM), https://www.washingtonpost.com/technology/2022/07/16/racist-robots-ai/ [https://perma.cc/2WFV-4DG3].

205. Alex Engler, *Auditing employment algorithms for discrimination,* Brookings (Mar. 16, 2021), https://www.brookings.edu/research/auditing-employment-algorithms-for-discrimination/ [https://perma.cc/XZ4P-H4WL].

206. These are groups of people legally protected from discrimination based on certain characteristics in U.S. law. They include race, color, religion or creed, national origin or ancestry, sex (including gender, sexual orientation, and gender identity), pregnancy, childbirth, and related medical conditions, age, physical or

of these laws have clarified that such discrimination will be prosecuted whether it is the result of analog decision-making or AI systems.

1. Housing

In June 2022, DOJ initiated its "first case challenging algorithmic bias under the Fair Housing Act."[207] Meta used a machine learning-powered targeting tool called a "Lookalike Audience" that enabled ads to target users "who share similarities with groups of individuals selected by an advertiser." The algorithm selected audiences in part using characteristics "including race, religion and sex."[208] As a result of the "Lookalike Audience" tool, Facebook users in certain protected groups did not receive housing ads.

The suit alleged the social media company violated the Fair Housing Act,[209] which prohibits discrimination in housing on the basis of protected characteristics, including race, color, national origin, religion, sex, familial status, and disability.[210] The DOJ argued that because "Meta uses algorithms in determining which Facebook users receive housing ads, and that those algorithms rely, in part, on characteristics protected under the FHA," the company should be held liable for disparate treatment and disparate impact discrimination.[211]

As part of the settlement, Meta agreed to stop using its Lookalike Audience tool in housing ads. Assistant Attorney General Kristen Clarke of the Justice Department's Civil Rights Division stated that "companies like Meta have a responsibility to ensure their algorithmic tools are not

---

mental disability, veteran status, genetic information, and citizenship. *Practical Law Glossary Item 5-501-5857*, WESTLAW, https://1.next.westlaw.com/Document/Ibb0a38daef0511e28578f7ccc38dcbee/View/FullText.html?transitionType=Default&contextData=(sc.Default)&firstPage=true&isplcus=true&bhcp=1 (last visited June 8, 2024).

207. Press Release, U.S. Dept. of Just., Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising, (June 21, 2022), https://www.justice.gov/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known [https://perma.cc/9JK8-UQNM].

208. *Id.*

209. 15 U.S.C. § 45 (2018), https://www.law.cornell.edu/uscode/text/42/chapter-45.

210. *Housing discrimination under the Fair Housing Act*, U.S. DEP'T OF HOUS. & URB. DEV., https://www.hud.gov/program_offices/fair_housing_equal_opp/fair_housing_act_overview [https://perma.cc/7K6Q-6SL3].

211. Press Release, U.S. Dept. of Just., Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising, (June 21, 2022), https://www.justice.gov/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known [https://perma.cc/9JK8-UQNM].

used in a discriminatory manner."[212] She added a warning that "[t]he Justice Department is committed to holding . . . technology companies accountable when they abuse algorithms in ways that unlawfully harm marginalized communities."[213]

Organizations using AI should take note that the DOJ has been clear on its intent to prosecute instances of disparate impact or other forms of discrimination against protected classes, regardless of whether the user of an AI system had intent or knowledge of such discrimination.

2. Hiring and Recruitment

In 2021, the EEOC announced the launch of an initiative focused on employment-related AI and other technological tools' compliance with federal civil rights laws.[214] As part of the initiative, the EEOC provided technical guidance, identified promising practices, held listening sessions, and gathered information about employment-related technologies. Since then, the EEOC has published guidance on employment laws under its purview[215] in addition to the historic joint statement with other federal regulatory bodies, announcing their commitment to using their legal authorities to prosecute discrimination from automated systems.[216]

This initiative led to the EEOC suit against iTutorGroup—a company offering online, remote tutoring to thousands of individuals—and its affiliates, alleging its online recruiting software was programmed to automatically reject older applicants for tutor positions in violation of the Age Discrimination in Employment Act ("ADEA").[217] The complaint aimed to secure back pay and liquidated damages for over

212. *Id.*
213. *Id.*
214. U.S. Equal Emp. Opportunity Comm'n, *Artificial Intelligence and Algorithmic Fairness Initiative*, https://www.eeoc.gov/ai [https://perma.cc/MLD5-QQUV].
215. U.S. Equal Emp. Opportunity Comm'n, Select Issues: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964, https://www.eeoc.gov/laws/guidance/select-issues-assessing-adverse-impact-software-algorithms-and-artificial [https://perma.cc/WP2C-K5SB]; U.S. Equal Emp. Opportunity Comm'n, The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees [hereinafter The Americans with Disabilities Act], https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence [https://perma.cc/P5G5-26XC].
216. Chopra, *supra* note 41.
217. Annelise Gilbert, *EEOC Settles First-of-Its-Kind AI Bias in Hiring Lawsuit (1)*, Bloomberg L. (Aug. 10, 2023, 9:21 AM), https://news.bloomberglaw.com/daily-labor-report/eeoc-settles-first-of-its-kind-ai-bias-lawsuit-for-365-000 [https://perma.cc/AVM2-K3GZ]; *see also* Press Release, U.S. Equal Emp. Opportunity Comm'n, EEOC

200 applicants who were denied jobs due to their age. It also sought injunctive relief to address and prevent future age discrimination.[218] According to the August 2023 consent decree filed in the U.S. District Court for the Eastern District of New York, iTutorGroup will pay a total gross sum of $365,000, to be distributed to applicants rejected on the basis of age and was enjoined from screening out future applicants on the basis of age.[219]

Companies using AI should take note that the EEOC also recently published its Draft Strategic Enforcement Plan ("SEP") for 2023–2027, which provides that the agency will focus on AI recruitment practices that discriminatorily "target job advertisements, recruit applicants, or make or assist in hiring decisions where such systems intentionally exclude or adversely impact protected groups."[220]

The EEOC is not the only federal agency monitoring recruitment practices. In June 2022, the DOJ signed settlements with 16 employers charged with using recruitment algorithms that discriminated against non-US citizens in violation of the Immigration and Nationality Act ("INA").[221] The INA anti-discrimination provision prohibits discrimination on the basis of citizenship status and national origin in firing, hiring, recruitment, or referral in exchange for a fee; it also prohibits unfair document-related requests, retaliation, and intimidation.[222] The settlements netted $832,944 in penalties against the employers, with individual employers paying as much as over $300,000.[223]

Sues iTutor Group for Age Discrimination, (May 5, 2022), https://www.eeoc.gov/newsroom/eeoc-sues-itutorgroup-age-discrimination [https://perma.cc/6D7K-EZ5D].

218. Press Release, U.S. Equal Emp. Opportunity Comm'n, EEOC Sues iTutor Group for Age Discrimination, (May 5, 2022), https://www.eeoc.gov/newsroom/eeoc-sues-itutorgroup-age-discrimination [https://perma.cc/6D7K-EZ5D].

219. Joint Notice of Settlement and Request for Approval and Execution of Consent Decree, Equal Emp. Opportunity Comm'n v. iTutor Group, Inc., No. 1:22-cv-2565 (E.D.N.Y. Feb. 9, 2023), https://www.bloomberglaw.com/public/desktop/document/EqualEmploymentOpportunityCommissionviTutorGroupIncetalDocketNo12/1?doc_id=X4663TFVFDF9ONAA8CMUJFPH3HR.

220. Draft Strategic Enforcement Plan, 88 Fed. Reg. 1379 (Jan. 10, 2023), https://www.federalregister.gov/documents/2023/01/10/2023-00283/draft-strategic-enforcement-plan.

221. Press Release, U.S. Dept. of Just., Justice Department Secures Settlements with 16 Employers for Posting Job Advertisements on College Recruiting Platforms That Discriminated Against Non-U.S. Citizens (June 27, 2022), https://www.justice.gov/opa/pr/justice-department-secures-settlements-16-employers-posting-job-advertisements-college [https://perma.cc/6J2H-QZZ4].

222. *Types of Discrimination*, U.S. Dep't of Just., Civ. Rts. Div. (Jan. 18, 2017), https://www.justice.gov/crt/types-discrimination [https://perma.cc/RAB8-MH9A].

223. Press Release, U.S. Dept. of Just., Justice Department Secures Settlements with 16 Employers for Posting Job Advertisements on College Recruiting Platforms That Discriminated Against Non-U.S. Citizens (June 27, 2022), https://www.justice.

Another legal avenue agencies have employed to contest AI-related discrimination is Title VII of the Civil Rights Act of 1964. In May 2023, the EEOC published guidance on select issues concerning Title VII and AI.[224] Title VII generally prohibits employment discrimination by disparate treatment based on race, color, religion, sex (including pregnancy, sexual orientation, and gender identity), or national origin.[225] The EEOC adopted the Uniform Guidelines on Employee Selection Procedures ("Guidelines") in 1978 to provide a framework for employers to determine whether their test and selection processes were permissible under Title VII. In a document released in May 2023, the EEOC clarified that these guidelines apply to algorithmic decision-making tools, and liability can be incurred if these tools have an impermissible adverse impact on a protected group, even if the tool was developed by a third party.[226]

Even before this guidance was issued, a lawsuit had been filed alleging an AI system violated rights protected by Title VII. In February 2023, representative plaintiff Derek Mobley filed a potential class action suit alleging that Workday, Inc., an HR software and management services provider, used discriminatory AI systems and screening tools.[227] Specifically, the suit alleges that the company's AI disproportionately disqualified applicants by race, age, and disability in violation of Title VII, the ADEA, and the ADA Amendments Act of 2008. The plaintiff claimed that, since 2018, he had applied to as many as one hundred jobs that use the hiring system and had been denied every time.[228]

Plaintiffs have also challenged AI employment practices on constitutional grounds. In *Hous. Fed'n of Tchrs. v. Hous. Indep. Sch. Dist.,*[229] a 2017 case, teachers in the Houston Independent School District were terminated after being rated "ineffective" by a privately

---

gov/opa/pr/justice-department-secures-settlements-16-employers-posting-job-advertisements-college [https://perma.cc/6J2H-QZZ4].

224. U.S. Equal Emp. Opportunity Comm'n, Select Issues: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964, https://www.eeoc.gov/laws/guidance/select-issues-assessing-adverse-impact-software-algorithms-and-artificial [https://perma.cc/WP2C-K5SB].

225. *Id.*

226. *Id.*

227. *U.S. District Court, California Northern District (San Francisco), Civil Docket for Case #: 3:23-cv-00770-RFL, Mobley v. Workday, Inc.*, Bloomberg L. (Feb. 21, 2023), https://www.bloomberglaw.com/public/desktop/document/MobleyvWORKDAYINCDocketNo423cv00770NDCalFeb212023CourtDocket/1?doc_id=X1Q6OIP7THO2 [https://perma.cc/BJ94-PCDR].

228. Complaint at 10–15, Mobley v. Workday, Inc., 3:23-cv-00770 (N.D. Cal.).

229. Hous. Fed'n of Tchrs., Loc. 2415 v. Hous. Indep. Sch. Dist., 251 F. Supp. 3d 1168 (S.D. Tex. 2017).

developed algorithm. Citing trade secrets, the company refused to divulge the algorithm, even to the school district, despite challenges by the teachers and teacher's union.[230] The court, however, was persuaded by the plaintiff's argument that due process requires that the teachers have the opportunity to test the validity of the school district's evaluation on their own behalf. Because the court found that the district did not provide sufficient information to allow the teachers to independently verify their scores,[231] it concluded that the school district had deprived them of their constitutionally protected property interest in their jobs.[232]

Given the risks of discrimination through AI tools, companies should conduct due diligence on AI tools prior to deployment to reduce bias and potential legal liability. For example, in 2018, Amazon decided to discard an AI hiring tool it had been building since 2014 after finding the program was irreparably biased against women.[233] The algorithm had been trained to vet job candidates based on resumes received over a historical ten-year period and, given the prevalence of successful male applicants who had been previously hired, the recruitment tool learned to penalize female candidates.[234] Amazon's decision to abort prior to deploying the AI system demonstrated prudent judgment and helped it to avoid legal, reputational, and ethical risks.

On May 12, 2022, the EEOC and DOJ issued first-of-its-kind joint guidance acknowledging that employers risk violating the Americans with Disabilities Act ("ADA") if they rely on algorithmic decision-making tools that "screen out" (whether intentionally or not) individuals with disabilities, or if they fail to provide reasonable accommodations for disabled applicants to be rated fairly by the hiring algorithm.[235] The guidance makes clear that an employer can be responsible under the ADA for its AI tool use, even if another entity designed or developed the technology.

The guidance provides examples of how AI use can violate the ADA.[236] For instance, a chatbot could be programmed to filter

230. *Id*. at 1177.

231. Valentine, *supra* note 191, at 373.

232. Ultimately, the parties settled the suit. American Federation of Teachers, *Federal Suit Settlement: End of Value-Added Measures for Teacher Termination in Houston* (Oct. 10, 2017), https://www.aft.org/press-release/federal-suit-settlement-end-value-added-measures-teacher-termination-houston [https://perma.cc/XPV2-EWPK].

233. Dastin, *supra* note 33.

234. *Id.*

235. The Americans with Disabilities Act, *supra* note 215; U.S. Dep't of Just., Civ. Rts. Div., *Algorithms, Artificial Intelligence, and Disability Discrimination in Hiring*, ADA.gov (May 12, 2022), https://www.ada.gov/resources/ai-guidance/ [https://perma.cc/4978-P6FA].

236. The Americans with Disabilities Act, *supra* note 215.

out applicants who indicate they have significant time gaps in their employment history. If these gaps are related to a disability, this action may violate the ADA. Similarly, video interviewing software that uses AI to evaluate candidates by finding patterns in their speech and facial expressions may not comply with legally required accommodations for certain disabilities (e.g., speech impediments) and thus could run afoul of the ADA.[237]

The EEOC and DOJ joint guidance on disability rights considerations when employing AI systems highlights the importance of. anticipating how individuals with disabilities might interact with the AI products.[238]

3. Discriminatory Practices under ECOA and FCRA

The FTC and CFPB regulate AI-enhanced credit decisions for discriminatory impact under two main statutes: the Equal Credit Opportunity Act ("ECOA") and the Fair Credit Reporting Act ("FCRA"). Recent FTC and CFPB publications demonstrate that these organizations are committed to enforcing regulations regarding discriminatory use of AI in credit decisions.[239]

Pursuant to ECOA, it is "illegal for a company to use a biased algorithm that results in credit discrimination on the basis of race, color, religion, national origin, sex, marital status, age, or because a person receives public assistance."[240] The law is referenced by FTC guidance on AI,[241] as well as by FTC Commissioners Bedoya and Slaughter and CFPB Director Chopra.[242] Declaring that "[c]ompanies are not absolved

237. The Americans with Disabilities Act, *supra* note 215; Joe Dysart, *Using AI and Video to Make Job Interviews More Efficient*, Transp. Topics (Sept. 8, 2023, 11:00 AM), https://www.ttnews.com/articles/using-ai-for-job-interviews [https://perma.cc/Q3AZ-VJMZ]; Jane Hanson, *AI Is Replacing Humans In The Interview Process – What You Need To Know To Crush Your Next Video Interview*, Forbes (Oct. 2, 2023, 6:57 PM), https://www.forbes.com/sites/janehanson/2023/09/30/ai-is-replacing-humans-in-the-interview-processwhat-you-need-to-know-to-crush-your-next-video-interview/?sh=c9e67051add3 [https://perma.cc/W62E-FE29].

238. The Americans with Disabilities Act, *supra* note 215.

239. Jillson, *supra* note 43; Consumer Fin. Prot. Bureau, Consumer Financial Protection Circular 2022-03 (May 26, 2022) [hereinafter *Consumer Financial Protection Circular*], https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/ [https://perma.cc/ZA9W-5W6F] (CFPB).

240. Jillson, *supra* note 43.

241. *Id.*

242. Bedoya, *supra* note 40 (Bedoya); Slaughter, *supra* note 43 (Slaughter); Newsroom, Consumer Fin. Prot. Bureau, CFPB Acts to Protect the Public from Black-Box Credit Models Using Complex Algorithms (May 26, 2022), https://www.consumerfinance.gov/about-us/newsroom/cfpb-acts-to-protect-

of their legal responsibilities when they let a black-box model make lending decisions," Chopra clarified, "[t]he law gives every applicant the right to a specific explanation if their application for credit was denied," and "*that right is not diminished simply because a company uses a complex algorithm that it doesn't understand*."[243]

Similarly, under FCRA, the FTC can investigate Consumer Report Agencies ("CRAs") that improperly use AI "to deny people employment, housing, credit, insurance, or other benefits."[244] Commissioner Slaughter explained that under FCRA, like ECOA, consumers are entitled to adverse action notices that can be contested, and CRAs must "apply reasonable procedures to ensure maximum possible accuracy when preparing consumer reports."[245] FTC guidance provides that, when deploying algorithms, companies should ensure that their decisions and actions are transparent, explainable, and fair[246] and, ultimately, that "data and models are robust and empirically sound."[247]

4. Workers' Rights

Understanding and advising clients on the appropriate use of algorithms in the workplace—particularly in the gig economy[248]—could raise questions pertaining to civil rights, employment, and consumer protection laws.[249]

Algorithmic wage discrimination, which disproportionately impacts low-income and marginalized workers, can lead to unpredictable and individualized pay scales.[250] As University of California law

---

the-public-from-black-box-credit-models-using-complex-algorithms/ [https://perma.cc/GRX8-Y8RP] (Chopra).

243. *Consumer Financial Protection Circular*, *supra* note 239 (Chopra) (emphasis added).

244. Jillson, *supra* note 43.

245. Slaughter, s*upra* note 43.

246. Andrew Smith, *Using Artificial Intelligence and Algorithms*, FED. TRADE COMM'N BUS. BLOG (Apr. 8, 2020), https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms [https://perma.cc/NX8E-7AD9].

247. *Id.*

248. Kathryn Taylor, *Gig Companies Are Manipulating Their Workers. Dark Patterns Laws Should Step In*, N.Y.U. J. OF LEGIS. & PUB. POL'Y (Feb. 7, 2023), https://nyujlpp.org/quorum/taylor-dark-patterns-laws/ [https://perma.cc/2V8U-86E7]; *see also* Megan Cerullo, *How companies get inside gig workers' heads with "algorithmic wage discrimination"*, CBS NEWS (Apr. 18, 2023, 4:34 PM), https://www.cbsnews.com/news/algorithmic-wage-discrimination-artificial-intelligence/ [https://perma.cc/M5BB-Z9X3].

249. Zephyr Teachout, *Surveillance Wages: A Taxonomy*, L. & POL. ECON. PROJECT (Nov. 6, 2023), https://lpeproject.org/blog/surveillance-wages-a-taxonomy/ [https://perma.cc/2YW6-2AAN].

250. Cerullo, *supra* note 248.

professor Veena Dubal explains, this dynamic results in workers being paid different rates for doing the same work.[251] Seeking legal recourse, three plaintiffs filed an antitrust complaint in California seeking to enjoin Uber and Lyft from, among other things, using a compensation system that employs "hidden algorithms" as opposed to a per-mile, per-minute, or per-trip pay system.[252] The plaintiffs argued that these companies exploited their duopolistic power to implement opaque payment systems in violation of California's unfair competition laws.[253] These and similar lawsuits will be instructive in determining if and how "gig economy" employers will adapt their use of algorithms to facilitate matters of compensation and workflow.

Pending federal legislation suggests that some policymakers want to provide more regulation and oversight. For example, Senator Ed Markey (D-Mass.) and Representative Doris Matsui (CA-06) introduced bicameral legislation to prohibit algorithms that discriminate on the basis of protected characteristics, address content amplification, and create an interagency task force to investigate discriminatory algorithmic processes across the economy.[254]

In May 2024, Colorado became the first state to implement comprehensive AI regulation when Governor Polis signed the "Concerning Consumer Protections in Interactions with Artificial Intelligence Systems," ("the Colorado AI Act").[255] The Colorado AI Act, which will go into effect in 2026, prohibits algorithmic discrimination and establishes requirements for developers and deployers of high-risk AI systems. The bill further institutes disclosure requirements for all AI systems to notify users when they are interacting with an artificial intelligence system.[256]

Laws calling for similar audits or regulation of AI technology have been proposed in states including Illinois, Maryland, New Jersey,

---

251. A. Martínez, *When your boss is an algorithm*, NPR (Apr. 25, 2023, 7:57 AM), https://www.npr.org/transcripts/1171800324#:~:text=Uber%20and%20Lyft%20drivers%20say%20those%20apps%20promote%20wage%20discrimination,that%20don't%20pay%20enough [https://perma.cc/3GMR-SSJP].

252. Complaint, Gill v. Uber Technologies, Inc., No. CGC22600284, ¶ 13 (Cal. Super. Ct. June 21, 2022).

253. *Id*.

254. Press Release, Sen. Ed Markey, Senator Markey, Rep. Matsui Introduce Legislation To Combat Harmful Algorithms And Create New Online Transparency Regime (May 27, 2021), https://www.markey.senate.gov/news/press-releases/senator-markey-rep-matsui-introduce-legislation-to-combat-harmful-algorithms-and-create-new-online-transparency-regime.

255. 2024 Colo. Sess. Laws 1199.

256. *Id*.

and California.[257] Many of these bills would seek to regulate not only companies that develop AI but also those that use AI tools in their day-to-day operations. A California bill introduced on January 30, 2023, AB 331, mandates that entities using automated decision tools ("ADT") for significant decisions must perform annual impact assessments detailing the ADT's purpose, benefits, and uses.[258] Another California bill, AB 302, proposes requiring inventories of high-risk ADTs used by state agencies.[259]

At a local level, in 2023, the Stop Discrimination by Algorithms Act ("SDAA") was reintroduced to the DC Council.[260] This bill aimed to prohibit deployers of automated decision-making systems from making discriminatory determinations in "important life decisions." For such determinations, the SDAA would require those who deploy AI to provide notice of how users' information is utilized, establish auditing requirements, and provide for both an agency and private right of action against violators. Importantly, this bill builds on protections afforded by the DC Human Rights Act.[261]

As with consumer protection laws, existing civil rights laws provide a framework to address AI-related harms. In order to address current gaps, both actual and perceived, AI discrimination continues to be the subject of numerous new bills, from curbing facial recognition technology to AI transparency proposals in the federal, state, and local

257. Jeffrey Bosley et al., *Employers Using AI in Hiring Take Note: Illinois' Artificial Intelligence Video Interview Act Is Now in Effect*, JDSUPRA (Feb. 11, 2020), https://www.jdsupra.com/legalnews/employers-using-ai-in-hiring-take-note-54767/ [https://perma.cc/A6YG-LE64]; Adam Forman & Nathaniel Glasser, *New Maryland Law Requires Applicant Consent Prior To Using Facial Recognition Technology In Job Interviews*, JDSUPRA (July 10, 2020), https://www.jdsupra.com/legalnews/new-maryland-law-requires-applicant-50746/ [https://perma.cc/7TKM-5Q6N]; G.A. 5430, 218th Leg., Reg. Sess. (N.J. 2019), https://www.billtrack50.com/BillDetail/1127840; Danielle Ochs et al., *California's Draft Regulations Spotlight Artificial Intelligence Tools' Potential to Lead to Discrimination Claims*, THE NAT'L L. REV. (May 13, 2022), https://natlawreview.com/article/california-s-draft-regulations-spotlight-artificial-intelligence-tools-potential-to [https://perma.cc/Z983-AWH6].

258. S.A. 331, 2023–24 Leg., Reg. Sess. (Cal. 2023). The assessments must be submitted to the Civil Rights Department within sixty days. Before using ADTs, those deploying AI must inform individuals about their use and accommodate requests for alternative decision-making methods, provided such requests are feasible. The bill prohibits ADTs that contribute to algorithmic discrimination and includes a clause allowing a private right of action against ADT users. AB 331 would also mandate that developers and deployers of automated decision tools conduct impact assessments of the tools in use, with noncompliance resulting in substantial administrative fines. The bill further requires that deployers inform individuals when such a tool is employed in making consequential decisions and provide an alternative selection process if feasible.

259. S.A. 302, 2023–24 Leg., Reg. Sess. (Cal. 2023).

260. D.C. B25-0114, 25th Council (D.C. 2023).

261. *Id.*; D.C. CODE §§ 2-140.01–.05 (1977).

governments.[262] The current climate of legislative and regulatory focus on algorithmic discrimination underscores the need for companies and counsel to assess and mitigate harm that could arise from using AI systems in the employment, housing, credit and advertising spaces, among others based on precedent on the books and articulated by federal agency leadership.

III. Privacy Considerations

Privacy laws like the Children's Online Privacy Protection Act ("COPPA") and the Health Insurance Portability and Accountability Act ("HIPAA") are being invoked to address the new forms of privacy harms that emerge from AI development and use. Privacy protection in the U.S. takes the form of various sector-specific laws combined with several comprehensive state laws. Because one of the key elements of AI systems is data, which can include personal data, privacy laws currently serve as a crucial mechanism for regulating AI systems. As such, privacy requirements and related potential liability at the federal, state, and global levels must be considered. This section focuses on how privacy law intersects with the use and regulation of AI across different jurisdictions, beginning by detailing existing federal privacy laws, including the Gramm-Leach-Bliley Act ("GLBA"), the Fair Credit Reporting Act ("FCRA"), the Family Educational Rights and Privacy Act ("FERPA"), the Electronic Communications Privacy Act ("ECPA"), and the Video Privacy Protection Act ("VPPA"). The section will also examine potential AI-related liabilities under COPPA and HIPAA in particular, and discuss ongoing efforts to establish a comprehensive federal data privacy law. The section concludes by exploring examples of state privacy laws in California, Colorado, Connecticut, and Virginia.

A. Privacy and AI Under Federal Law

In contrast to the General Data Protection Regulation ("GDPR") in Europe, the U.S. does not currently have a comprehensive federal privacy law to regulate data use.[263] Instead, there are a number of U.S. federal privacy laws that address privacy concerns, as listed above.[264] This subsection examines how AI systems can incur liability under two of those laws—COPPA and HIPAA—and explores the recent push to create a comprehensive federal data privacy law.

---

262. *Ban Facial Recognition*, *supra* note 159.

263. *See infra* Global Considerations for more details on GDPR.

264. Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. Times: Wirecutter (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ [https://perma.cc/8R37-TMCR].

1. COPPA

Under COPPA, operators of websites or services are subject to additional requirements when their content is "directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age."[265] This law is enforced through the FTC's Children's Online Privacy Protection Rule ("COPPR").[266]

COPPA "requires that child-directed websites, apps, and other online services provide notice of their information practices and obtain verifiable parental consent before collecting personal information from children under thirteen, including the use of persistent identifiers to track a user's internet browsing habits for targeted advertising."[267] That requirement also applies to certain third parties "where they have actual knowledge they are collecting personal information directly from users of child-directed websites and online services."[268]

A complaint filed in 2022 by the DOJ on behalf of the FTC illustrates the serious legal penalties that can occur when companies' AI use violates child data privacy laws.[269] In *United States v. Kurbo, Inc.*, the government argued that WW International, formerly Weight Watchers, and its subsidiary were marketing a weight-loss application to children as young as eight years old and illegally collecting their personal information.[270] In addition to imposing a $1.5 million penalty, the settlement order required the company "to delete personal information illegally collected from children under 13 [and] destroy any algorithms derived from the data."[271]

COPPA will likely continue to generate significant litigation as children become internet-savvy at younger ages and employ online tools

265. Children's Online Privacy Protection Rule, 89 Fed. Reg. 2034, 2034 (Jan. 11, 2024); *see also* Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506, https://uscode.house.gov/view.xhtml?path=/prelim@title15/chapter91&edition=prelim; 16 C.F.R. § 312 (2000), https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa.

266. 16 C.F.R. § 312 (2000), https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa.

267. Slaughter, *supra* note 43.

268. *Id.*

269. Complaint, United States v. Kurbo, Inc., 22-CV-946 (N.D. Cal. 2022).

270. Press Release, Fed. Trade Comm'n, FTC Takes Action Against Company Formerly Known as Weight Watchers for Illegally Collecting Kids' Sensitive Health Data (Mar. 4, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-company-formerly-known-weight-watchers-illegally-collecting-kids-sensitive [https://perma.cc/328R-V44D].

271. *Id.*

for numerous daily tasks and purposes, both educational and social. A stipulated order between the FTC, DOJ and Amazon illustrates this trend. The order, filed in May 2023 and entered by the court in July 2023, requires Amazon to pay a $25 million fine and delete data it has retained on children (voice recordings, geolocation information, etc.).[272] In a policy statement published last year, the FTC reiterated its intent to prosecute education technology companies which illegally use data involving or belonging to children.[273] And, in January 2024, the FTC published a notice of proposed rulemaking to strengthen protections of children's online data by reinforcing data minimization, updating methods and levels of parental consent, addressing advertisements and engagement tactics, bolstering data security and more.[274]

2. HIPAA

HIPAA is a federal law governing protection of healthcare data.[275] This law's numerous protections include:[276] a privacy rule,[277]

272. Federal Trade Commission, Proposed Stipulated Order for Amazon.com, Inc., FTC File No. 1923128, Docket No. 2-1, at 1 (filed June 1, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/Amazon-Proposed-Stipulated-Order-%28Dkt.-2-1%29.pdf; Press Release, Fed. Trade Comm'n, FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests (May 31, 2023) [hereinafter *Alexa Charges*], https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever [https://perma.cc/8C9G-A2MB]; Press Release, U.S. Dept. Justice, Amazon Agrees to Injunctive Relief and $25 Million Civil Penalty for Alleged Violations of Children's Privacy Law Relating to Alexa (July 19, 2023), https://www.justice.gov/opa/pr/amazon-agrees-injunctive-relief-and-25-million-civil-penalty-alleged-violations-childrens.

273. Press Release, Fed. Trade Comm'n, FTC to Crack Down on Companies that Illegally Surveil Children Learning Online (May 19, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-crack-down-companies-illegally-surveil-children-learning-online. As an example of government attention, Samuel Levine, director of the FTC's Bureau of Consumer Protection, has explicitly highlighted that companies may not use children's data to train their algorithms. *See Alexa Charges*, *supra* note 272 ("COPPA does not allow companies to keep children's data forever for any reason, and certainly not to train their algorithms.").

274. Children's Online Privacy Protection Rule, 89 Fed. Reg. 2034 (proposed Jan. 11, 2024).

275. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 100 Stat. 2548 (1996), https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996.

276. Off. for Civ. Rts., *HIPAA for Professionals*, U.S. Dep't of Health & Hum. Servs. (May 17, 2021), https://www.hhs.gov/hipaa/for-professionals/index.html [https://perma.cc/H2H7-HK9P].

277. Off. for Civ. Rts., *The HIPAA Privacy Rule*, U.S. Dep't of Health & Hum. Servs. (June 7, 2024), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html [https://perma.cc/V7LB-CERV].

a security rule,[278] an enforcement rule,[279] an omnibus rule (which provides strengthened privacy and security protections),[280] and a breach notification[281] rule.[282] Health care providers, and entities processing data on their behalf, that violate HIPAA are liable for penalties exceeding $60,000 for each violation, up to an annual penalty limit of over $2 million.[283]

Dinerstein v. Google, a 2019 lawsuit brought against Google, demonstrates how a company's use of AI could generate liability if it fails to properly consider HIPAA requirements. The case featured a breach of contract claim, which alleged that the University of Chicago Medical Center violated HIPAA by sharing information with Google.[284] The University of Chicago Medical Center had announced in 2017 that it was partnering with Google to find ways to improve health care by studying electronic medical records.[285] Although both the Medical Center and Google confirmed that the health data was de-identified

278. Off. for Civ. Rts., *The Security Rule*, U.S. Dep't of Health & Hum. Servs. (Oct. 20, 2022), https://www.hhs.gov/hipaa/for-professionals/security/index.html [https://perma.cc/E37R-Q3QD].

279. Off. for Civ. Rts., *The HIPAA Enforcement Rule*, U.S. Dep't of Health & Hum. Servs. (Aug. 31, 2020), https://www.hhs.gov/hipaa/for-professionals/special-topics/enforcement-rule/index.html [https://perma.cc/A5CM-WWMB].

280. Off. for Civ. Rts., U.S. Dep't of Health & Hum. Servs., Omnibus HIPAA Rulemaking (Sept. 13, 2019), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/omnibus-hipaa-rulemaking/index.html [https://perma.cc/P5XF-AYUY].

281. Off. for Civ. Rts., *Breach Notification Rule*, U.S. Dep't of Health & Hum. Servs. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html [https://perma.cc/6TL2-QDJH].

282. The HIPAA Privacy Rule regulates how covered entities and related business associations "address the use and disclosure of individuals' health information," with the aim of balancing the protection of personal health information against allowing disclosures necessary for providing adequate health care. Business associations include "organization[s], other than a member of a covered entity's workforce," that perform "certain functions or activities on behalf of, or provide certain services to, a covered entity that involve the use or disclosure of individually identifiable health information" including data analysis. The Security Rule "establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity."

283. This is based on the 2023 inflation rate table. *What Are the Penalties for HIPAA Violations?*, HIPAA Journal (May 1, 2023), https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/ [https://perma.cc/3AS3-8FLK].

284. Class Action Complaint & Demand for Jury Trial at 2, Dinerstein v. Google, LLC, 484 F. Supp. 3d 561 (N.D. Ill. 2020) [hereinafter Class Action Complaint], *aff'd as modified*, 73 F.4th 502 (7th Cir. 2023).

285. Evan Sweeney, *Academic medical centers team up with Google to bolster machine learning and predictive analytics*, Fierce Healthcare (May 22, 2017), https://www.fiercehealthcare.com/analytics/academic-medical-centers-team-up-google-for-analytics-support.

before being used[286] (using data that is sufficiently de-anonymized is permissible under HIPAA[287]), the plaintiff argued that the information could be re-identified through AI.[288]

Although the complaint was dismissed for failing to establish damages, large tech companies' continued reliance on health data in their AI training and use has led observers to call for and lawmakers to explore stronger data privacy protections.[289]

3. Proposals for a Comprehensive Federal Data Privacy Law

The federal patchwork of sector-specific data privacy laws has resulted in numerous gaps. Many politicians and experts continue to call for a comprehensive federal data privacy law,[290] which could serve as an important precursor or complement to AI legislation.[291] In April 2023, President Biden urged Congress to pass "bipartisan privacy legislation that, one, impose[s] strict limits on personal data that tech companies collect on all of us; two, ban[s] . . . targeted advertising to children; and

286. Heather Landi, *Lawsuit accuses University of Chicago of sharing identifiable patient data with Google*, FIERCE HEALTHCARE (Jan. 27, 2019), https://www.fiercehealthcare.com/tech/lawsuit-accuses-university-chicago-sharing-patient-data-google.

287. U.S. Dep't of Health & Hum. Servs., Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (July 13, 2013), https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html.

288. Class Action Complaint, *supra* note 284; Latanya Sweeney, *Matching Known Patients to Health Records in Washington State Data* (Inst. for Quantitative Soc. Sci., Data Priv. Lab, Working Paper), https://dataprivacylab.org/projects/wa/1089-1.pdf; Linda Carroll, *Anonymous patient data may not be as private as previously thought*, YAHOO NEWS (Dec. 21, 2018), https://news.yahoo.com/anonymous-patient-data-may-not-private-previously-thought-190248280.html; Hazel Tang, *The risks of de-identified and re-identified data*, A.I. IN MED. (Apr. 23, 2020), https://ai-med.io/ai-in-medicine/the-risks-of-de-identified-and-re-identified-data/.

289. Jenna Becker, *Insufficient Protections for Health Data Privacy: Lessons from Dinerstein v. Google*, BILL OF HEALTH (Sept. 28, 2020), https://blog.petrieflom.law.harvard.edu/2020/09/28/dinerstein-google-health-data-privacy/; Mohana Ravindrath, *Lawmakers call for HIPAA updates following Google's data deal*, POLITICO (Nov. 15, 2019), https://www.politico.com/news/2019/11/15/lawmakers-call-for-hipaa-updates-following-googles-data-deal-071088.

290. Joe Biden, *Republicans and Democrats, Unite Against Big Tech Abuses*, WALL ST. J. (Jan. 11, 2023), https://www.wsj.com/articles/unite-against-big-tech-abuses-social-media-privacy-competition-antitrust-children-algorithm-11673439411?mod=hp_opin_pos_3#cxrecs_s; Joseph Duball, *U.S. House lawmakers keep federal privacy legislation top of mind*, IAPP (Mar. 1, 2023), https://iapp.org/news/a/us-house-lawmakers-keep-federal-privacy-legislation-top-of-mind/.

291. Cameron F. Kerry, *How privacy legislation can help address AI*, BROOKINGS (July 7, 2023), https://www.brookings.edu/articles/how-privacy-legislation-can-help-address-ai/.

three, require[s] companies to put health and safety first in the products that they build."[292]

Numerous privacy bills have been proposed in recent years.[293] The American Data Privacy and Protection Act ("ADPPA") is considered a front-runner in the ongoing efforts to create a national law.[294] The bill, which advanced to the full House of Representatives in July 2022, features a novel approach to preemption of state privacy laws with exceptions for specific categories of state laws,[295] including data breach notification laws, the preservation of certain privacy laws in Illinois and California, and the creation of a private right of action.[296] It has not been reintroduced this session as of the date of this publication,[297] and it remains unclear whether ADPPA, or a similar bill, will ultimately pass.

B. Privacy Under State Law

In addition to use-specific privacy laws, such as the biometric laws discussed in Section II.A, several states have enacted data privacy laws that regulate how their residents' data is processed and protected. Currently, thirteen states—California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, Oregon, Tennessee, Texas,

---

292. *President Biden Meets with Council of Advisers on Science and Technology*, C-SPAN (Apr. 4, 2023), https://www.c-span.org/video/?527170-1/president-biden-meets-council-advisers-science-technology; https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/04/04/remarks-by-president-biden-in-meeting-with-the-presidents-council-of-advisors-on-science-and-technology/.

293. Müge Fazlioglu, *U.S. Federal Privacy Legislation Tracker*, IAPP, https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/ (last visited Mar. 24, 2024); Jonathan M. Gaffney et al., Cong. Rsch. Serv., LSB10776, Overview of the American Data Privacy and Protection Act, H.R. 8152 (2022), https://crsreports.congress.gov/product/pdf/LSB/LSB10776.

294. *American Data Privacy and Protection Act Topic Page*, IAPP, https://iapp.org/resources/topics/adppa/ (last visited July 8, 2024) ("The proposed ADPPA and its legislative path are the closest U.S. Congress has ever been to passing comprehensive federal privacy legislation.").

295. *Id*.

296. *Id.* (Other key provisions of the bill include its coverage of most entities, with additional requirements for certain service providers; its application to data that identifies individuals; and its establishment of duties of loyalty for covered entities largely limiting the collection, use, and transfer of covered data, except for specific purposes. Additionally, the bill emphasizes transparency, consumer control and consent, and protecting for individuals under the age of seventeen. It also imposes obligations on third-party data collection entities, includes civil rights and algorithmic discrimination protections, and mandates data security practices.) Gaffney et al., *supra* note 293.

297. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/house-bill/8152/all-actions?q=%7B%22search%22%3A%22%5C%22American+Data+Privacy+and+Protection+Act%5C%22%22%7D&s=2&r=1&overview=closed#tabs.

Utah, and Virginia—have enacted comprehensive data privacy laws.[298] This section provides a brief overview of those laws, touching on four of those thirteen states, to illustrate some of the legal requirements that institutions should be mindful of when using AI to process data.

The California Consumer Privacy Act ("CCPA") statute, enacted in 2018 and operational since January 2020,[299] includes notable protections, such as the "right to know" (consumers can "request that businesses disclose what personal information they have collected, used, shared, or sold"); the "right to delete" (consumers have the right to request deletion of their personal data held by businesses); the "right to opt out" (i.e., of the sale of their own data by a business); and nondiscrimination (businesses cannot discriminate against consumers for exercising their CCPA rights).[300]

AI companies often rely on large datasets that could include personal information to train and improve their algorithms. Therefore, the requirement to disclose information and potentially delete data at a consumer's request introduces operational challenges for AI systems already in use and potentially limits the amount of data available for future AI development.[301]

In 2020, California voters approved amendments to the CCPA in a ballot initiative known as the California Privacy Rights Act ("CPRA").[302] This amendment established the right to correct information and to limit use and disclosure of sensitive personal information. It also clarified and updated requirements for businesses' use of data, including retention, minimization, limitation, and the processing of deletion requests.[303]

298. *US: 2023 Models of State Privacy Legislation*, BSA (Sept. 19, 2023), https://www.bsa.org/policy-filings/us-2023-models-of-state-privacy-legislation.

299. CAL. CIV. CODE § 1798.100–199.100 (2023).

300. *CCPA and CPRA Topic Page*, IAPP, https://iapp.org/resources/topics/ccpa-and-cpra/ (last visited Mar 24, 2024); *California Consumer Privacy Laws,* BLOOMBERG L., https://pro.bloomberglaw.com/brief/california-consumer-privacy-laws-ccpa-cpra/ (last visited Mar. 24, 2024); *Laws & Regulations*, CAL. PRIV. PROT. AGENCY, https://cppa.ca.gov/regulations/ (last visited Mar. 24, 2024); Maria Korolov, *California Consumer Privacy Act (CCPA): What you need to know to be compliant*, CSO (July 7, 2020), https://www.csoonline.com/article/565923/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html.

301. Some scholars have argued that deleting the data is not enough to comply due to the "imprint" that data leaves on the AI system and that algorithmic destruction is a possible alternative or supplemental remedy. *See* Tiffany C. Li, *Algorithmic Destruction*, 75 SMU L. REV. 479 (2022), https://scholar.smu.edu/smulr/vol75/iss3/2/.

302. *California Privacy Rights Act (CPRA)*, PERKINS COIE, https://www.perkinscoie.com/en/practices/security-privacy-law/california-privacy-rights-act-cpra.html (last visited Mar. 24, 2024); *California Consumer Privacy Laws*, *supra* note 300.

303. *Id.*

After the Colorado Attorney General's Office published final rules for implementing the Colorado Privacy Act ("CPA"), a comprehensive law protecting consumers' personal data went into effect on July 1, 2023.[304] The rules outline the responsibilities of these businesses, known as "controllers," which include providing transparent privacy notices, avoiding deceptive user interfaces ("dark patterns"), and conducting rigorous data protection assessments.[305] Notably, the CPA stipulates a universal opt-out mechanism, allowing consumers to refuse the processing of their data for targeted advertising or sales, with the relevant provisions becoming effective on July 1, 2024.[306]

The Connecticut Data Privacy Act ("CTDPA"),[307] enacted in 2022, applies to businesses operating within the state or providing services to its residents that process personal data or assist in doing so.[308] The act covers "processors" and "controllers" that handle personal data, though nonprofits, financial institutions, and government bodies are exempt.[309] The CTDPA grants consumers several rights, including access to personal data, the ability to correct inaccuracies, and the option to opt out of targeted advertising. Businesses must adhere to data security measures, limit data collection, and obtain consent before processing sensitive data, among other obligations. The Connecticut Attorney General enforces the CTDPA with potential penalties up to $5,000 per willful violation, restitution, and injunctive relief.[310] Starting on January 1, 2025, the attorney general will have discretionary authority to provide opportunities to cure based on a six-factor test.[311]

---

304. CO. CODE § 6-1-1301–1313 (2022); *Colorado Privacy Act,* OFF. OF THE ATT'Y GEN., COLO. DEPT. OF L., https://coag.gov/resources/colorado-privacy-act/.

305. CO. Code § 6-1-1303.

306. F. Paul Pittman et al., *Colorado Privacy Act Rules Finalized Ahead of July 1, 2023 Effective Date*, WHITE & CASE (Apr. 14, 2023), https://www.whitecase.com/insight-alert/colorado-privacy-act-rules-finalized-ahead-july-1-2023-effective-date.

307. CONN. GEN. STAT. § 42-515-525 (2023); *Bill Status: Substitute for S.B. No. 6, Session Year 2022,* CONN. GEN. ASSEMB., https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB00006&which_year=2022 [https://perma.cc/U6RB-A9XE].

308. *Connecticut Data Privacy Act—What Businesses Need to Know*, AKIN GUMP (May 26, 2024), https://www.akingump.com/en/insights/alerts/connecticut-data-privacy-act-what-businesses-need-to-know (last visited Mar. 24, 2024).

309. CONN. GEN. STAT. § 42-515 (2023).

310. AKIN GUMP, *supra* note 308.

311. An Act Concerning Personal Data Privacy and Online Monitoring, Conn. Pub. Act No. 22-15, (2023). The six factors are: "(1) the number of violations; (2) the size and complexity of the controller or processor; (3) the nature and extent of the controller's or processor's processing activities; (4) the substantial likelihood of injury to the public; (5) the safety of persons or property; and (6) whether such alleged violation was likely caused by human or technical error." *Id.*

Illinois's Artificial Intelligence Video Interview Act mandates that employers notify and obtain consent from applicants when AI is used to analyze video interviews and that they explain how the AI functions.[312] The law has been modified to require employers exclusively using AI tools to report the race and ethnicity of candidates to the Illinois Department of Commerce and Economic Opportunity annually,[313] facilitating state analysis of potential AI-induced racial biases.

The Virginia Consumer Data Protection Act ("VCDPA"), signed into law in March 2021, provides Virginians with rights to access and delete their personal data.[314] The law requires businesses to carry out data protection assessments for targeted advertising and sales activities, and an exception to the right to delete exists for data collected from sources other than the consumer.[315] Businesses are required to ensure systems are in place to safeguard these VCDPA rights.[316]

Introduced and passed in Montana in May 2023, the Consumer Data Privacy Act seeks to regulate the collection and processing of personal data, as well as automated decision-making which uses this data.[317] The bill emphasizes transparency around profiling, allowing individuals to opt out of automated decisions that have significant effects on them. In the bill, profiling is described as automated processing of personal data to assess various attributes of an individual. Moreover, for profiling that contains a heightened risk of harm, a data protection assessment is mandated for controllers.[318] The bill indicates that processing that presents a heightened risk of harm to a consumer includes: the processing of personal data for the purposes of targeted advertising; the sale of personal data; the processing of personal data for profiling, in which the profiling presents a reasonably foreseeable risk of unfair or deceptive treatment of, or unlawful disparate impact on, consumers; financial, physical, or reputational injury to consumers; a physical or other form of intrusion on the solitude, seclusion, or private affairs of consumers in which the intrusion would be offensive to a reasonable

312. 820 Ill. Comp. Stat. 42 (2020), https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=4015&ChapterID=68.
313. *Id.*
314. Va. Code § 59.1-575-585 (2021); Sarah Rippy, *Virginia passes the Consumer Data Protection Act*, IAPP (Mar. 3, 2021), https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/.
315. Va. Code § 59.1-575-585 (2021).
316. *Virginia Consumer Data Protection Act* (VCDPA), Bloomberg L., https://pro.bloomberglaw.com/brief/virginia-consumer-data-protection-act-vcdpa/ (last visited Mar. 24, 2024).
317. MT. Code § 30-14-2801-2817 (2023), https://leg.mt.gov/bills/2023/billpdf/SB0384.pdf.
318. *Id.*

person; other substantial injury to consumers; and the processing of sensitive data.[319]

Municipalities have also stepped in to regulate AI. New York City's Local Law 144, which went into effect on July 5, 2023,[320] regulates automated decision-making tools ("AEDT") and prohibits employers from deploying AEDTs if they fail to conduct annual bias tests of those tools. The law also imposes reporting requirements regarding the bias audits and mandates certain notices to employees and job applicants.[321]

Given that AI systems generally require vast amounts of information to learn and make decisions, its development and use raises significant privacy concerns and compliance challenges under numerous legal frameworks. The evolving landscape of privacy law in the United States presents a patchwork of federal and state regulations that influence how AI is regulated. At the federal level, laws like COPPA and HIPAA govern specific aspects of AI data use and protection. Recent cases such as *United States v. Kurbo, Inc.*[322] underscore the significant legal penalties companies can face for AI-related violations of child data privacy laws, while *Dinerstein v. Google*[323] highlights the importance of considering HIPAA requirements in AI applications involving health data. Moreover, the push for a comprehensive federal data privacy law, exemplified by proposed legislation like the American Data Privacy and Protection Act, reflects some recognition of the limitations of current regulatory frameworks in addressing the challenges posed by AI. Meanwhile, at the state level, the emergence of comprehensive data privacy laws in states like California, Colorado, Connecticut, and Virginia introduces additional obligations for businesses utilizing AI. Some of these laws grant consumers the right to control their personal data and impose strict requirements on data processing practices. Overall, these developments highlight the increasing importance of considering privacy implications in the deployment of AI technologies.

IV. Intellectual Property

Generative AI, though still in its early stages, poses numerous legal questions in the field of copyright law regarding the creation of

319. *Id.*

320. *Automated Employment Decision Tools (AEDT)*, NYC Consumer & Worker Prot., https://www.nyc.gov/site/dca/about/automated-employment-decision-tools.page.

321. *Id.*

322. United States of America v. Kurbo, Inc. et al, 3:22-cv-00946, 6 (N.D. Cal. Feb. 16, 2022).

323. Dinerstein v. Google, LLC, 484 F. Supp. 3d 561 (N.D. Ill. 2020), *aff'd as modified*, 73 F.4th 502 (7th Cir. 2023).

copyrightable works and the limits of training AI systems on copyrighted materials. With the development and expanding use of content-generating programs, such as Chat-GPT, Bard, and DALL-E, questions as to the relationship between AI and copyright will continue to arise.[324] This section delves into the intersection of AI and intellectual property, specifically focusing on copyright law that lawyers and executives should consider when developing or deploying AI. It examines the criteria for copyrightable work, initially addressing whether AI-generated materials qualify for copyright protection, including the current stance of the U.S. Copyright Office and its enforcement of the "human authorship" requirement. Subsequently, it explores the use of copyrighted works in AI training, discussing the application of the fair use doctrine and how it pertains to incorporating copyrighted content into AI training processes.

A. Establishing Copyrightable Work

In February 2023, the U.S. Copyright Office clarified that AI-generated material is not copyrightable, stating that it will not register works that are "produced by a machine or mere mechanical process," including work "without any creative input or intervention from a human author."[325]

The Copyright Office's stance is premised on a fundamental tenet of federal copyright law that "A work must be created by a human being."[326] In December 2022, the Copyright Office applied this concept to AI-generated material when it denied an attempt by computer scientist Stephen Thaler to copyright an image he had created with an algorithm called Creativity Machine.[327] Thaler argued that Creativity

---

324. Ellen Sheng, *In generative AI legal Wild West, the courtroom battles are just getting started*, CNBC (Apr. 3, 2023), https://www.cnbc.com/2023/04/03/in-generative-ai-legal-wild-west-lawsuits-are-just-getting-started.html.

325. Letter from Robert J. Kasunic, Assoc. Reg. of Copyrights & Dir. of Registration Pol'y & Prac. at U.S. Copyright Off., to Kristina Kashtanova (Oct 28, 2022), https://copyright.gov/docs/zarya-of-the-dawn.pdf [https://perma.cc/GJ7E-58WC].

326. U.S. Copyright Office, Compendium of U.S. Copyright Office Practices § 313.2 (3d ed. 2021), https://www.copyright.gov/comp3/chap300/ch300-copyrightable-authorship.pdf; Thaler v. Vidal, No. 21-2347 (Fed. Cir. 2022). With regard to models that use databases and datasets, while data itself is not copyrightable in the US, databases in their entirety can be protected by copyright as a compilation. However, the mere collection of data is not sufficient to trigger copyright protection under the law. The arrangement and selection of data must be sufficiently creative or original. *See* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340 (1991).

327. Letter from Shira Perlmutter, et al., Reg. of Copyrights at U.S. Copyright Off. Rev. Bd., to Ryan Abbott, Esq., Brown, Neri, Smith & Khan, LLP (Feb. 14, 2022), https://www.copyright.gov/rulings-filings/review-board/docs/a-recent-entrance-to-paradise.pdf.

Machine should be recognized as an independent author and that the image belonged to him as a work for hire.[328] A D.C. District Court judge upheld the Copyright Office's decision, agreeing that "human authorship is a bedrock requirement of copyright."[329]

There are various possible outcomes to U.S. legal treatment of AI-created works. First, AI works may be deemed to lack authorship and therefore to fall into the public domain.[330] Alternatively, if preexisting creative works were used to train the AI, a court could find the resulting AI-generated work derivative of those other works—meaning that owners of the preexisting works could sue others for potential copyright infringement.[331] A "derivative work" can be based on one or more existing works and is protected by the original copyright, entitling the original copyrighted work's owner to bring an infringement suit for unauthorized use.[332] In addition, the owner of the subsequent AI-created derivative work could claim copyright protection for what is deemed to be "new" or original aspects of the derivative work.[333]

The limits of "human authorship" were recently tested when artist Kristina Kashtanova applied for copyright approval for her comic book *Zaraya of the Dawn*, created using Midjourney, a generative AI tool.[334] In February 2023, the U.S. Copyright Office affirmed the requirement of human authorship but also indicated that AI-assisted works could still fall within that category.[335] In this case, the Copyright Office concluded that Kashtanova was the author of the work's text, selection, coordination, and arrangement of its written and visual elements, but

328. *See* Thaler v. Vidal, No. 21-2347, at 7 (Fed. Cir. 2022).

329. Wes Davis, *AI-generated art cannot be copyrighted, rules a U.S. federal judge*, THE VERGE (Aug. 19, 2023), https://www.theverge.com/2023/8/19/23838458/ai-generated-art-no-copyright-district-court; Thaler v. Perlmutter, No. 22-1564, Mem. Op. (D.D.C 2023).

330. Schuyler Moore, *The Implications Of AI Elements Not Being Protected By Copyright*, FORBES (Aug. 31, 2023), https://www.forbes.com/sites/schuylermoore/2023/08/31/the-implications-of-ai-elements-not-being-protected-by-copyright/?sh=530ecc5d2c80.

331. Gil Appel et al., *Generative AI Has an Intellectual Property Problem*, HARV. BUS. REV. (Apr. 7, 2023), https://hbr.org/2023/04/generative-ai-has-an-intellectual-property-problem.

332. Edward A. Haman, *What are derivative works under copyright law?*, LEGALZOOM (Mar. 22, 2023), https://www.legalzoom.com/articles/what-are-derivative-works-under-copyright-law.

333. U.S. COPYRIGHT OFFICE, CIRCULAR 14: COPYRIGHT IN DERIVATIVE WORKS AND COMPILATIONS (2020), at 2, https://www.copyright.gov/circs/circ14.pdf.

334. *See* Kasunic, *supra* note 325.

335. Letter from Robert J. Kasunic, Assoc. Reg. of Copyrights & Dir. of Registration Pol'y & Prac. at U.S. Copyright Off., to Van Lindberg, Taylor English Duma LLP (Feb. 21, 2023) https://copyright.gov/docs/zarya-of-the-dawn.pdf [https://perma.cc/P948-FD56].

because the individual images generated by Midjourney were not produced by a human, they were not separately copyrighted.[336] Thus, under this precedent, the use of generative AI could render the work not protected under copyright, regardless of an author or artist's efforts to select, coordinate, or arrange work.[337] Moreover, the Copyright Office will not grant a copyright if the work presents ambiguity in the roles of creation. In September 2023, artist Jason Allen failed in his own copyright bid for his AI-assisted artwork *Théâtre D'opéra Spatial* due to his refusal to disclaim the substantial AI-generated content in his application.[338]

There remains an unresolved and critical question regarding whether there is a meaningful distinction between works that are created *by* AI and works created with the *assistance* of AI. The Copyright Office has said that an AI-generated work could be an original work if a human were to "select or arrange AI-generated material in a sufficiently creative way."[339] However, it did not specify what makes a particular way of selecting or arranging material "sufficiently creative" under the law. Consider a user who enters creative prompts into DALL-E to generate an image. If the user inserts the prompts into the program, would that count as "creative input" from a human "author"? And if the user then modifies the prompt to revise the image, would that count as "intervention"?

On December 12, 2022, the Copyright Office, responding to a letter from two U.S. senators, stated that it intends to examine these issues more closely.[340] It also agreed, depending on funding, to consider a request to establish a national commission on AI.[341]

336. *Id.*; Copyright Registration Guidance: Containing Material Generated by Artificial Intelligence, 88 Fed. Reg. 16190 (Mar. 16, 2023) (to be codified at 37 C.F.R. pt. 202) [hereinafter Copyright Registration Guidance], https://copyright.gov/docs/zarya-of-the-dawn.pdf.

337. *See id.*

338. Letter from Suzanne V. Wilson, Gen. Counsel and Assoc. Reg. of Copyrights at U.S. Copyright Off., et. al., to Tamara S. Pester, Tamara S. Pester, LLC (Dec. 5, 2023), https://www.copyright.gov/rulings-filings/review-board/docs/Theatre-Dopera-Spatial.pdf.

339. Copyright Registration Guidance, *supra* note 336.

340. Letter from Kathi Vidal, Dir. of the U.S. P.T.O., & Shira Perlmutter, Dir. of the U.S. Copyright Off., to Thom Tillis, U.S. Sen., & Chris Coons, U.S. Sen. (Dec. 12, 2022), https://www.copyright.gov/laws/hearings/Letter-to-USPTO-USCO-on-National-Commission-on-AI-1.pdf [https://perma.cc/Y5C2-LKND].

341. *Id.*

B. Liability from Use of Copyrighted Works in Training Data

Another area of potential liability under copyright law involves the use of copyrighted materials in the training of AI and whether using existing works to train AI triggers claims of copyright infringement.

Several recent lawsuits have highlighted potential liability that can be triggered in the development and use of generative AI, including two class actions against Stability AI and one against Microsoft.[342] High-profile actors and authors, such as Sarah Silverman,[343] George R.R. Martin, Jodi Picoult, and John Grisham,[344] among others, have brought suits against OpenAI for allegedly copying their work without permission to train AI models. To successfully demonstrate a copyright infringement, these suits will need to establish that the AI program had access to the copyright material and that the output is "substantially similar" to it.[345]

Companies have been consistently pushing the boundaries of copyright laws in their quest for data to train their AI systems.[346] Incorporating existing creative works or other forms of content into AI models for training purposes often involves creating a copy of that content.[347] OpenAI has acknowledged that its process for training AI

342. Joseph Saveri L. Firm LLP, *Class Action Filed Against Stability AI, Midjourney, and DeviantArt for DMCA Violations, Right of Publicity Violations, Unlawful Competition, Breach of TOS*, PR NEWSWIRE (Jan. 14, 2023, 3:51 PM), https://www.prnewswire.com/news-releases/class-action-filed-against-stability-ai-midjourney-and-deviantart-for-dmca-violations-right-of-publicity-violations-unlawful-competition-breach-of-tos-301721869.html [https://perma.cc/X9ZS-V66L]; Preston Gralla, *This lawsuit against Microsoft could change the future of AI*, COMPUTERWORLD (Jan. 10, 2023), https://www.computerworld.com/article/3684734/this-lawsuit-against-microsoft-could-change-the-future-of-ai.html.

343. Matt O'Brien, *Sarah Silverman and novelists sue ChatGPT-maker OpenAI for ingesting their books*, AP NEWS (July 12, 2023, 2:56 PM), https://apnews.com/article/sarah-silverman-suing-chatgpt-openai-ai-8927025139a8151e26053249d1aeec20 [https://perma.cc/X65W-P3TU].

344. Emilia David, *George R.R. Martin and other authors sue OpenAI for copyright infringement*, THE VERGE (Sept. 2023, 11:03 AM), https://www.theverge.com/2023/9/20/23882140/george-r-r-martin-lawsuit-openai-copyright-infringement.

345. CHRISTOPHER T. ZIRPOLI, CONG. RSCH. SERV., LSB10922, GENERATIVE ARTIFICIAL INTELLIGENCE AND COPYRIGHT LAW 4 (2023). In at least two cases, courts have rejected claims for failing to demonstrate substantial similarity. Will Oremus & Elahe Izadi, *AI's future could hinge on one thorny legal question*, WASH. POST (Jan. 4, 2024), https://www.washingtonpost.com/technology/2024/01/04/nyt-ai-copyright-lawsuit-fair-use.

346. *See* Cade Metz et al., *How Tech Giants Cut Corners to Harvest Data for A.I.*, N.Y. TIMES (Apr. 6, 2024), https://www.nytimes.com/2024/04/06/technology/tech-giants-harvest-data-artificial-intelligence.html.

347. In the process of ingesting information for training data, models make downloaded, digital copies (not necessarily permanent copies). From the copyright

models "involves first making copies of the data to be analyzed."[348] The answer of whether this activity is protected may turn on courts' interpretation of the "fair use" doctrine of copyright law.

The fair use doctrine promotes "freedom of expression by permitting the unlicensed use of copyright-protected works in certain circumstances,"[349] using a balancing test set out in Section 107 of the Copyright Act.[350] The test, applied on a case-by-case basis, considers four factors: (1) the use's purpose and character, e.g. commercial or nonprofit educational; (2) the work's nature; (3) the quantity and substantiality of the portion used in relation to the entire copyrighted work; and (4) the impact on the potential market for or value of the copyrighted work.[351] At its core, fair use requires courts to consider the policy interests served by making the derivative work available to the public, and to weigh those benefits against the interest of the original work's owner in being able to enforce their copyright.

OpenAI has taken the position that its use of existing content to train its AI models falls under fair use and is therefore exempt from liability.[352] The company argues that it uses existing content only for the purpose of creating new content and that this makes its use of the original content "transformative" rather than merely copying the original work.[353] Additionally, OpenAI contends that its use of existing content does not share that content with the public in a way that would involve taking credit for it—in other words, it is neither competing with nor threatening the original creator's ability to benefit from those works.[354] Despite these arguments, works produced by generative AI systems could be seen as market substitutes for the original works, which is a factor that courts weigh when determining if the fair use doctrine applies.[355] Other companies have advanced an alternative "fair learning" approach, which would offer limited fair use protection when

---

owner's perspective, this can seem like copyright infringement, because under the Copyright Act, they have exclusive right to make copies of their works.

348. OpenAI, LP, Comment Regarding Request for Comments on Intellectual Property Protection for Artificial Intelligence Innovation, at 2 (2019), https://www.uspto.gov/sites/default/files/documents/OpenAI_RFC-84-FR-58141.pdf.

349. *U.S. Copyright Office Fair Use Index*, COPYRIGHT.GOV (last updated Nov. 2023), https://www.copyright.gov/fair-use.

350. Copyright Act § 107, 17 U.S.C. § 107.

351. *U.S. Copyright Office Fair Use Index*, *supra* note 349.

352. OpenAI, LP, *supra* note 348, at 5.

353. *Id.* at 4–9.

354. *Id* at 10–12.

355. *U.S. Copyright Office Fair Use Index*, *supra* note 349.

training AI models for "non-expressive" purposes that do not run afoul of copyright laws.[356]

Nearly a decade ago, fair use doctrine was a successful defense in *Authors Guild v. Google, Inc.*, in which authors sued the tech giant for scanning digital copies of their books and making the resulting search function available to the public, characterizing Google's actions as "copyright infringement on an epic scale."[357] The Second Circuit disagreed, finding that "Google's unauthorized digitizing of copyright-protected works, creation of a search functionality, and display of snippets from those works are non-infringing fair uses."[358] Moreover, the court determined that the copying "is highly transformative, the public display of text is limited, and the revelations do not provide a significant market substitute for the protected aspects of the originals."[359]

More recently, a group of artists filed suit against Stability AI, the creator and operator of the Stable Diffusion AI image generator, for "download[ing] or otherwise acquir[ing] copies of billions of copyrighted images without permission," which were used to train the Stable Diffusion system.[360] Getty Images filed suit against Stability AI the following month for "unlawfully cop[ying] and process[ing] millions of images protected by copyright and the associated metadata" without a license, "owned or represented by Getty Images[,] . . . to benefit Stability AI's commercial interests."[361] Getty's suit alleges that Stability AI scraped over 12 million images, which it used to train models and create synthetic images in violation of copyright protections.[362] A related proposed class action suit was filed in November 2022 against Microsoft and OpenAI over their AI-assisted coding tool GitHub

356. Mark A. Lemley & Bryan Casey, *Fair Learning*, 99 TEX. L. REV., 4 (2021), https://texaslawreview.org/fair-learning/.

357. Authors Guild v. Google, Inc., *cert denied*, No. 15-849 (Dec. 31, 2016); *see also* Authors Guild v. Google, Inc., 804 F.3d 202 (2d Cir. 2015).

358. Authors Guild v. Google, Inc., 804 F.3d at 229.

359. *Id.* at 229.

360. Complaint & Demand for Jury Trial at 1, Andersen v. Stability AI Ltd., No. 23-CV-00201 (N.D. Cal. Jan. 13, 2023); James Vincent, *AI art tools Stable Diffusion and Midjourney targeted with copyright lawsuit*, THE VERGE (Jan. 16, 2023, 6:28 AM), https://www.theverge.com/2023/1/16/23557098/generative-ai-art-copyright-legal-lawsuit-stable-diffusion-midjourney-deviantart.

361. *Getty Images Statement*, GETTYIMAGES (Jan. 17, 2023), https://newsroom.gettyimages.com/en/getty-images/getty-images-statement; *see also* Complaint & Demand for Jury Trial, Getty Images, Inc. v. Stability AI, Inc. (D. Del. Feb. 3, 2023), https://copyrightlately.com/pdfviewer/getty-images-v-stability-ai-complaint.

362. Complaint & Demand for Jury Trial, Getty Images, Inc. v. Stability AI, Inc., ¶ 8 (D. Del. Feb. 3, 2023).

Copilot.[363] The suit alleges that the coding assistant application engaged in "software piracy on an unprecedented scale" by reproducing long sections of licensed code without attributing credit.[364]

There continues to be ambiguity surrounding the application of the fair use doctrine to AI systems, and courts have suggested that these cases are highly fact-dependent. In September 2023, a U.S. district court held that a jury trial was needed to determine whether a search engine developer could claim fair use protection for copying summaries of court cases from Westlaw, a well-known legal research company, in order to train an AI program.[365]

These suits could have significant implications for the development and regulation of AI systems. The utility of AI models is strongly tied to the efficacy and robustness of the datasets upon which they are trained.[366] Accurate, reliable recommendations require sufficient and representative data from which to draw conclusions, given that AI systems are essentially learning to predict desired outputs based on prior determinations and patterns identified in the training data.[367] Therefore, if courts rule that copyrighted works cannot be included in training datasets without explicit permission, a potential second-order consequence would be a dramatic increase in the barriers to developing robust algorithms in light of the cost, feasibility, and other challenges to obtaining such permission(s).

The U.S. Supreme Court recently reexamined the fair use doctrine in Andy Warhol Foundation for the Visual Arts v. Goldsmith.[368] In a 7-2 decision, the Court ruled that the Andy Warhol Foundation ("AWF") infringed on Lynn Goldsmith's copyright to her 1981 photograph of the artist Prince. Goldsmith had originally licensed the image to Vanity

363. James Vincent, *The lawsuit that could rewrite the rules of AI copyright*, THE VERGE (Nov. 8, 2022, 11:09 AM), https://www.theverge.com/2022/11/8/23446821/microsoft-openai-github-copilot-class-action-lawsuit-ai-copyright-violation-training-data.

364. *Id.*; Complaint & Demand for Jury Trial, Doe v. Github, Inc., No. 22-CV-06823 (N.D. Cal. Nov. 3, 2022).

365. Thomson Reuters Enter. Ctr. GmbH v. Ross Intel. Inc., No. 20-CV-613-SB, 2023 WL 6210901 (D. Del. Sept. 25, 2023).

366. Katharine Miller, *Data-Centric AI: AI Models Are Only as Good as Their Data Pipeline*, STAN. UNIV. HUM.-CENTERED A.I. (Jan. 25, 2022), https://hai.stanford.edu/news/data-centric-ai-ai-models-are-only-good-their-data-pipeline [https://perma.cc/TUP7-XUC5].

367. Joe McKendrick, *Artificial Intelligence Without The Right Data Is Just … Artificial*, FORBES (Dec. 30, 2022, 4:15 PM), https://www.forbes.com/sites/joemckendrick/2022/12/30/artificial-intelligence-without-the-right-data-is-just-artificial.

368. Andy Warhol Found. for Visual Arts, Inc. v. Goldsmith, 598 U.S. 508 (2023).

Fair for a one-time use.[369] In 2016, AWF licensed Warhol's Orange Prince, which was based on Goldsmith's photograph, to Vanity Fair, prompting Goldsmith to claim copyright infringement. The majority, while acknowledging that there are fair uses of copyrighted works, concluded that Goldsmith's photograph and "AWF's copying use of that photograph in an image licensed to a special edition magazine devoted to Prince share substantially the same purpose, and the use is of a commercial nature."[370]

Lawmakers have proposed legislation responsive to copyright owners' concerns. For instance, Representative Don Beyer (D-VA-8) introduced the AI Foundation Model Transparency Act,[371] which calls on the FTC and the NIST to create guidelines for widely used foundation model deployers to publicize certain information about the model—such as how it was trained, how it performs on certain metrics, whether user data is collected, and details about the computational power that the foundation model uses to train and function.[372]

A bipartisan group of senators, Maria Cantwell (D-Wash.), Marsha Blackburn (R-Tenn.) and Martin Heinrich (D-N.M.) introduced the Content Origin Protection and Integrity from Edited and Deepfaked Media Act ("COPIED ACT") which would provide the owners of content the ability attach ownership information to their content and make it unlawful to for generative AI models to be trained on or produce content that has ownership information without the owner's consent.[373] Representative Adam Schiff (D-CA-30) also introduced the Generative AI Copyright Disclosure Act, which would require organizations that operate generative AI systems to submit notice to the U.S. Copyright Office regarding all copyrighted works used to train the AI system.[374]

The emergence of generative AI technologies has raised important legal questions about how to apply existing intellectual property laws.

---

369. *Id.* at 508.

370. *Id.* at 550.

371. H.R. 6881, 118th Cong. (2023).

372. One of the bill's core concerns reflects the increase in lawsuits and public concern about copyright infringement.

373. Press Release, U.S. Senate Committee on Commerce, Science, & Transportation, Cantwell, Blackburn, Heinrich Introduce Legislation to Increase Transparency, Combat AI Deepfakes & Put Journalists, Artists & Songwriters Back in Control of Their Content, (July 11, 2023) https://www.commerce.senate.gov/2024/7/cantwell-blackburn-heinrich-introduce-legislation-to-combat-ai-deepfakes-put-journalists-artists-songwriters-back-in-control-of-their-content [https://perma.cc/KV88-A54M].

374. *Rep. Schiff Introduces Groundbreaking Bill to Create AI Transparency Between Creators & Companies*, ADAM SCHIFF (Apr. 9, 2024), https://schiff.house.gov/news/press-releases/rep-schiff-introduces-groundbreaking-bill-to-create-ai-transparency-between-creators-and-companies.

Under current copyright law, the requirement of human authorship for copyright protection underscores the need to define the limits of AI assistance in human-created works—a question that will continue to be examined by the U.S. Copyright Office and the courts. The use of copyrighted materials in training AI models introduces additional legal complexities. The lawsuits around AI training data and copyright infringement generally come down to the question of the application of the fair use doctrine to AI systems. The courts' interpretations of the fair use doctrine and the balancing of interests between copyright holders and AI developers will significantly impact the development and regulation of AI technologies.

Given the open questions in AI copyright law, the Copyright Office has undertaken a study of the intersection between the technology and the law and solicited public comments to facilitate this examination.[375] As the Copyright Office continues to define the limits of human authorship and litigants battle over how far the fair use protection extends, legal practitioners should closely monitor developments in this rapidly evolving field. Clarifying the parameters of copyright protection and fair use in relation to AI will be essential to determining the rights of creators and copyright holders and may be an area for future legislation.

V. Contracts

The contracts supporting the development and deployment of AI—from self-driving cars[376] to hiring[377] and other employment decisions—create additional novel questions of potential liability. This section examines AI liability within contract law, considering how contracts could impact AI development and potential allocation of liability. This overview includes questions about how AI is classified under U.S. case law and the Uniform Commercial Code ("UCC"), as well as the risks in AI-assisted contract formation.

U.S. law has historically classified software as *both* a good and a service.[378] It remains unclear whether U.S. courts will categorize AI systems embedded in software products as goods. A violation of

375. Artificial Intelligence and Copyright, 88 Fed. Reg. 59942 (Aug. 30, 2023) (notice and request for comments).

376. *See generally*, Andrew Myers, *How AI Is Making Autonomous Vehicles Safer*, Stan. Univ. Hum.-Centered A.I. (Mar. 7, 2022), https://hai.stanford.edu/news/how-ai-making-autonomous-vehicles-safer.

377. *In Machines We Trust: A four-part investigation into automated hiring practices*, MIt Tech. Rev. (downloaded using https://forms.technologyreview.com/podcasts/in-machines-we-trust/).

378. Tanenbaum et al., *supra* note 101; Robert Dube, *So Good It's a Service: The Changing Legal Perspective on Computer Software*,

specified contractual conditions or warranties could lead to potential contractual liabilities for the AI user and/or the AI developer, including implied warranties of fitness for a particular purpose or inherent quality of the AI system. However, the level of software customization necessary to invoke the implied UCC warranty of fitness—the seller asserts the product is suitable for the buyer's purpose—remains an open question.[379]

All U.S. states and the District of Columbia have adopted portions of the UCC governing contract law.[380] Under the UCC, readily available software that incorporates an AI feature would likely be categorized as a "good."[381] The UCC requires that the related contract contain express warranties, as well as implied warranties of "merchantability,"[382] "fitness for a particular purpose,"[383] and assurance of valid title.[384] To mitigate their contractual liabilities, AI system developers may attempt to negate these warranties using disclaimers or more informal language.[385]

The proliferation of AI creates at least three potential implications under contract law that lawyers should consider in evaluating potential risk and liability. First, AI can lead to unsatisfactory bargaining. AI can automate contract creation, but it may fail to negotiate terms that align with human interests, leading to unsatisfactory or unintended outcomes. Second, there is the potential for AI-induced breach of contract. AI systems, due to programming errors or a failure to understand nuanced human contexts, might inadvertently cause a breach of contract, complicating liability determination. Third, limited AI comprehension can lead to unintended consequences. A lack of understanding of AI technologies or their implications could have high consequences for a deal, potentially leading to skewed contracts, subsequent disputes, and uneven understanding of possible harms and liabilities. The following subsections provide context on each of these three issues.

EKLAND & BLANCO (Nov. 17, 2021), https://www.ecklandblando.com/blog/2021/11/so-good-its-a-service-the-changing-legal-perspective-on-computer-software/ [https://perma.cc/9R4Y-6GC3].

379. 2 U.C.C. § 315, https://www.law.cornell.edu/ucc/2/2-315.

380. Commercial Law: Uniform Commercial Code (UCC), Georgetown Law Library (last updated June 2, 2023), https://guides.ll.georgetown.edu/commerciallaw/ucc.

381. *Id.*; Tanenbaum et al., *supra* note 101.

382. 2 U.C.C. § 314.

383. 2 U.C.C. § 315.

384. 2 U.C.C § 609.

385. OPENAI, *Terms of use*, https://openai.com/policies/terms-of-use (last visited Mar. 24, 2024).

A. Unsatisfactory Bargaining

U.S. law primarily handles electronic contracting under Section 14 of the Uniform Electronic Transactions Act ("UETA"),[386] which governs automated transactions.[387] This law addresses the emergence of AI-powered chatbots in contracts, enabling AI to assist in the procurement process,[388] negotiate and finalize[389] terms of a contract, and autonomously execute contractual obligations.[390]

Walmart's use of an AI chatbot in its procurement negotiations is illustrative of the application of the UETA to AI programs.[391] Walmart partnered with Pactum, a chatbot company, in 2021 to conduct a pilot program in Canada to use the chatbot to negotiate with eighty-nine of its suppliers.[392] Through this program, the chatbot closed deals with 64 percent of the suppliers, averaging eleven days per deal.[393] Walmart expanded the program to the United States, Chile, and South Africa, and in 2022, the chatbot closed deals with 68 percent of its suppliers.[394]

However, as with many other AI applications, the program was not without risk. Pactum's co-founder warned that chatbot-driven negotiations could "create harm" if the algorithms are given inaccurate information.[395] Additionally, Facebook researchers discovered that

386. Adopted by forty-nine states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands. New York has not adopted the UETA. *Glossary: Uniform Electronic Transactions Act (UETA)*, Thomson Reuters Prac. L., https://content.next.westlaw.com/practical-law/document/I66e3df587a6611e498db8b09b4f043e0/Uniform-Electronic-Transactions-Act-UETA?viewType=FullText&transitionType=Default&contextData=(sc.Default)#:~:text=The%20UETA%20has%20been%20adopted,and%20the%20US%20Virgin%20Islands.

387. Uniform Electronic Transactions Act §14 (1999). An open legal question attaches when using AI to enter into a legal contract: Has actual consent been provided by a party when AI uses dynamic and arguably unforeseen behavior to act on the party's behalf? To the authors' knowledge, no court has yet ruled on this issue. *See also* Huu Nguyen & Scott Bailey, *Use of Artificial Intelligence for Smart Contracts and Blockchains,* Fintech Law Report, March-Apr. 2018, at 2 (Apr. 2018).

388. Joe McKendrick, *Your Next Negotiating Partner: Artificial Intelligence*, Forbes (Mar. 17, 2023), https://www.forbes.com/sites/joemckendrick/2023/03/17/your-next-negotiating-partner-artificial-intelligence/?sh=6bd6f791605b.

389. "AI techniques useful for automatic negotiations and smart contract control include expert systems, search, neural networks, and the Minmax algorithm. If adequate consent has been given by the parties, AI could use these algorithms to negotiate as an electronic agent on behalf of the parties." Nguyen & Bailey, *supra* note 387, at 3.

390. *See generally id.* at 3.

391. McKendrick, *supra* note 388.

392. Katie Shonk, *Chatbot Negotiations: What Can AI Do for You?*, Harv. Program on Negot. Daily Blog (Dec. 19, 2023), https://www.pon.harvard.edu/daily/negotiation-skills-daily/chatbot-negotiations-what-can-ai-do-for-you/.

393. *Id.*

394. McKendrick, *supra* note 388.

395. Shonk, *supra* note 392.

negotiation chatbots have the potential to learn sophisticated negotiation tactics, including bluffing.[396] Their study showed that agents "learnt to deceive without any explicit human design, simply by trying to achieve their goals." This development raises concerns that AI chatbots could develop other techniques that violate ethical or legal boundaries.[397] While AI-facilitated contracting presents an opportunity for efficiency and standardization, the risk remains that in the absence of human input and oversight, this AI use could result in unintended, undesirable and even legal consequences.

"Smart contracts," which utilize blockchain technology to conduct self-executing agreements, are an example of automated transactions that rely on code.[398] Notably, these contracts must still meet a traditional contract's requirements, such as offer, acceptance, and consideration, to be legally enforceable,[399] while also offering benefits[400] such as expediency, transparency, and identifying user error and fraud.[401] One concern this AI use raises is whether these agreements are rigid by design and lack variety.[402] By integrating AI into their development, however, these contract negotiations can become more sophisticated, adapting to conditions, applying predictive analytics, and assisting in dispute resolution.[403] One company, Cortex, has already incorporated AI onto the blockchain by providing machine learning to support the

396. Steve LeVine, *Facebook unveils a chatbot that can bluff and negotiate*, AXIOS (June 16, 2017), https://www.axios.com/2017/12/15/facebook-unveils-a-chatbot-that-can-bluff-and-negotiate-1513303038.

397. Shonk, *supra* note 392.

398. *See* 21 No. 2 Fintech L. Rep. NL 1.

399. Jeffrey D. Neuburger et al., *Smart Contracts: Best Practices*, PROSKAUER ROSE: PRACTICAL L. (2019), https://blockchainandthelaw.proskauerroseblogs.com/wp-content/uploads/sites/9/019/11/Smart-Contracts-Best-Practices-w-022-2968.pdf. Some states have also taken the step to remove doubt of the enforceability of smart contracts. For example, in March 2018, Tennessee adopted a law that states: "Smart Contracts may exist in commerce. No contract relating to a transaction shall be denied legal effect, validity, or enforceability solely because that contract contains a Smart Contract term." Tenn. Code. Ann. § 47-10-201 and §47-10-202. Other states, including Arizona, Wyoming, Nevada, and Ohio, have adopted similar legislation.

400. *See* Cortex Labs, *AI Smart Contracts — The Past, Present, and Future*, MEDIUM (Dec. 6, 2018), https://medium.com/cortexlabs/ai-smart-contract-5018dc56e2d8.

401. For instance, Cook County, Illinois, is piloting a program to use blockchain technology to prevent fraudulent deed transfers. Lester Coleman, *Cook County to Use the Bitcoin Blockchain for Property Conveyance*, CCN (Mar. 4, 2021), https://www.ccn.com/cook-county-to-use-the-bitcoin-blockchain-for-property-conveyance/.

402. Brad Spannbauer, *AI meets blockchain: Revolutionizing smart contracts and cryptocurrency*, COIN TELEGRAPH (May 1, 2023), https://cointelegraph.com/innovation-circle/ai-meets-blockchain-revolutionizing-smart-contracts-and-cryptocurrency [https://perma.cc/XVL6-XL9H]; Cortex Labs, *supra* note 400.

403. Spannbauer, *supra* note 402.

adaptation of smart contracts to real-world cases.[404] It utilizes both the programming language Solidity and AI models to create the contracts.

Traditional contract law, grounded in principles of human consent and intent, must grapple with the implications of these autonomous contracts when disputes arise over agreements that do not reflect the parties' consent. For instance, an AI-supported software program contract that fails to execute a task required under the contract could result in a material breach. It is complicated to identify the responsible party in such situations, as the software is technically responsible for the offending action but the company that deployed that software did so with the inherent risks of utilizing this AI program. Alternatively, if the offending action is due to a coding error—and inconsistent with contract terms—the party losing the benefit of the bargain is deemed to own the liability.[405]

B. AI-Induced Breach of Contract

AI has already been implicated in breach of contract claims. In February 2023, the District Court for the Central District of California decided a breach-of-contract case involving social media influencers.[406] The defendant, Darkstore, originally reached out to an influencer marketing company, Influential Network, to promote Darkstore's same-day delivery app. After completion of the contract, Darkstore refused to pay, and Influential Network sued for breach of contract. Darkstore's CEO declared that "given that Plaintiff uses artificial intelligence generated look-alike influencers to trick customers into thinking that it is a real influencer when it is not, Plaintiff has not complied with its obligations under the Statement of Work."[407] The court deemed the defendant's claim meritless, stating that the use of such influencers, even if they were AI-generated, did not invalidate the plaintiff's performance. Additionally, the defendant previously approved these influencers and all agreed-upon terms were met, including the term that the content would reach between 50,000 and 150,000 people.

Another recent contract suit involved Meta and Shared.com, an online content creator. Shared.com used Meta applications to promote its content, both by purchasing ads and participating in a program that placed articles on Meta's news feed. Shared alleged that Meta did not

404. CORTEX, https://cortexlabs.ai/ [https://perma.cc/C6CM-68D4] (last visited Mar. 24, 2024).
405. Neuburger et al., *supra* note 399.
406. Influential Network, Inc. v. Darkstore, Inc., No. 2:21-cv-07162-AB-JEM (C.D. Cal. 2023).
407. *Id.* (citing Hnetinka Decl. at ¶ 16).

provide enough notice regarding rejected ads and articles, failed to submit a payment on time, and violated its terms of service by suspending Shared's Facebook pages.[408] In *Shared.com v. Meta Platforms, Inc.*, the court denied Meta's motion to dismiss, citing the unfair and fraudulent prongs of California's Unfair Competition Law ("UCL").[409] To establish compliance with the "unfair" prong of UCL, Shared alleged that Meta was "over-relian[t] on artificial intelligence" in ad regulation, which led them to sacrifice appropriate customer rejection explanations in an attempt to maximize profits. In considering whether Shared's claim about fraudulent business practices satisfied pleading standards, the court noted Meta's overreliance on AI, given that Meta "knew or should have known that it could not comply with [customers'] expectation[s] due to its averred reliance on artificial intelligence."[410]

C. Limited AI Comprehension

Nuance Communications, Inc. v. IBM serves as "a contemporary window into the brave new world of artificial intelligence ('AI') commercial applications."[411] In the case, Nuance and IBM entered into a software licensing agreement that provided Nuance with a copy of IBM's "Automatic Open-Domain Question Answering" software system and ten years of software updates. The disagreement that emerged between the parties related to the scope of the updates IBM was required to provide to Nuance.

The court found that IBM had breached its agreement with Nuance by failing to update to commercialize its well-known AI system[412] before it ultimately ruled in favor of IBM. The court found that Nuance had been willfully blind and failed to make appropriate inquiries to IBM about the breach. However, the plaintiff's claims were barred by the statute of limitations.

The contractual frameworks surrounding AI technology have notable implications for liability and legal compliance. Contracts in the

408. Shared.com v. Meta Platforms, Inc., 22-cv-02366-RS (N.D. Cal. Sept. 21, 2022), https://casetext.com/case/sharedcom-v-meta-platforms-inc.
409. *Id.*
410. *Id.*
411. Nuance Commc'n, Inc. v. Int'l Bus. Machines Corp., 544 F. Supp. 3d 353 (S.D.N.Y. 2021), https://casetext.com/case/nuance-communications-inc-v-international-business-machines-corp-1.
412. "While the parties did not intend to give Nuance access to all the natural language technology developed by IBM, their primary purpose was to give Nuance access to any updates to DeepQA that would facilitate Nuance's creating commercially applicable products directly from the DeepQA code (e.g., the blue-washed code)." *Nuance Commc'n*, 544 F. Supp. 3d at 371.

development and deployment of AI technologies not only define the terms of engagement between AI developers and users but delineate the boundaries of liability and responsibility. The UCC classification influences warranties and liability, particularly regarding standards of merchantability, fitness for a particular purpose, and the assurance of valid title.

AI-related programming errors or misinterpretation of human intentions could present additional contractual liabilities. While AI can streamline negotiations, there are risks of unsatisfactory outcomes if AI systems do not align with human interests or legal standards. For example, Walmart's use of AI chatbots in negotiations highlights both efficiency gains and potential risks of misunderstanding or unintended legal consequences. These issues are crucial not only for legal professionals but also policymakers and business leaders as their resolution will shape the future of AI development and its societal impact.

VI. AI Readiness and Policy Proposals

Following the preceding sections on legal doctrines that impact use and development of artificial intelligence, this section explores changes in AI readiness—the U.S. capacity to incorporate and regulate AI technology—as well as novel trends, authorities, regulatory regimes, and advisory bodies to be aware of as they further inform AI standards and best practices. The number of proposed federal AI bills more than doubled from 88 in 2022 to 181 in 2023.[413] There was also a 56.3% increase in the number of AI-related regulations.[414] That number is only going to increase as society's interest in and reliance on AI grows, particularly at the state level. In a recent study, a trade association found that state lawmakers proposed 440 percent more AI-related bills in 2023 than the year prior, with nearly 200 bills introduced.[415]

This section touches on efforts at the federal, state, and local levels to address AI, illustrating the significant uptick in legislative and regulatory interest in this technology. It examines, first, congressional action and policy proposals; second, Executive Branch initiatives, including the AI Executive Orders, OSTP's AI Bill of Rights, the National Artificial Intelligence Initiative Office ("NAIIO"), the National

413. Stan. Univ. Hum.-Centered A.I., 2024 AI Index Report, https://aiindex.stanford.edu/report/.

414. *Id.*

415. BSA, *BSA Analysis: State AI Legislation Surges by 440% in 2023* (Sept. 27, 2023), https://www.bsa.org/news-events/news/bsa-analysis-state-ai-legislation-surges-by-440-in-2023.

AI Advisory Committee ("NAIAC"), third, Commerce Department, State Department, Department of Defense/ Department of Homeland Security Initiatives and fourth, state and local government involvement.

A. Congressional Action

The following section explores the National Defense Authorization Act of 2019, which made key investments to enhance the United States' AI readiness. From the inception of the National Security Commission on Artificial Intelligence ("NSCAI") to the strategic advancements propelled by the National Artificial Intelligence Initiative Act of 2020, this section describes how the funds and new entities established in recent legislation are shaping America's technology and security landscape.

The National Defense Authorization Act ("NDAA") of 2019 established several key institutions and investments to increase the country's AI readiness.[416] For instance, the NDAA created the National Security Commission on Artificial Intelligence ("NSCAI") to provide findings and recommendations to the president and Congress on how best to address national security concerns and defense needs related to AI.[417]

The following year, Congress passed the National Artificial Intelligence Initiative Act of 2020 ("NAIIA"),[418] encompassed in the 2021 NDAA, which established the National Artificial Intelligence Initiative ("NAII") to ensure U.S. leadership in R&D, trustworthy development, and use of AI; prepare the U.S. workforce; and coordinate federal AI efforts.[419] The NAIIA also established the National Artificial Intelligence Initiative Office ("NAIIO") and the National AI Advisory Committee ("NAIAC"),[420] which is further outlined below. The NDAA continues to be a vehicle for AI development, as seen in the numerous AI provisions in the FY 2023 legislation[421] and FY 2024 bill.[422] Taken

416. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No 115-232 (Dec. 20, 2019).

417. *Final Report*, Nat'l Sec. Comm'n on A.I. (Oct. 5, 2021), https://cybercemetery.unt.edu/nscai/20211005220330/https://www.nscai.gov.

418. National Artificial Intelligence Initiative Act of 2020, H.R. Res. 6395, 116th Cong. (2020) (enacted).

419. *Id.* at § 5101.

420. For transparency, co-author Miriam Vogel serves as chair of NAIAC.

421. *Summary of AI Provisions from the National Defense Authorization Act 2023*, Stan. Univ. Hum.-Centered A.I. (last visited May 27, 2024) [hereinafter *Summary of AI Provisions*], https://hai.stanford.edu/summary-ai-provisions-national-defense-authorization-act-2023 [https://perma.cc/L4BV-HAQL].

422. Divyansh Kaushik et al., *FY24 NDAA AI Tracker*, Fed'n Am. Scientists (July 18, 2023), https://fas.org/publication/fy24-ndaa-ai-tracker [https://perma.cc/3973-N2NV].

together, these congressional actions underscore Congress's proactive role in shaping and advancing the nation's AI landscape.

Recent major government R&D investment in AI research and development and the CHIPS and Science Act (the "CHIPS Act")[423] could significantly impact the U.S. AI landscape. In 2022, the Biden administration worked with Congress to pass the CHIPS Act to, in part, strengthen the U.S. semiconductor chip supply.[424] Advanced semiconductors are a vital component of AI technology, and policies such as the CHIPS Act will impact how AI is developed and deployed in the U.S.[425] For example, within the various provisions of the CHIPS Act, there is an emphasis on collaboration with international partners to foster trust in "other emerging technologies," which may encompass AI.[426] The bill allots $9 billion in NIST to advance research and standards development for AI, as well as other future industries.[427] The bill also directs the NIST director to set up virtual "testbeds" intended for "the development of robust and trustworthy" AI technologies.[428]

B. Congressional Proposals

The U.S. Congress continues to signal interest in educating itself on and regulating AI. In 2023, Senate Majority Leader Chuck Schumer launched the AI Insight Forums, a nine-part series of closed-door hearings with leading AI experts to discuss issues ranging from copyright and innovation to privacy and risk management.[429] Nearly

423. Chips and Science Act, H.R.4346, 117th Cong. (2022) (enacted).

424. Press Release, White House, FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China (Aug. 9, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china [https://perma.cc/7BLQ-TKX4].

425. *What The CHIPS and Science Act means for Artificial Intelligence*, Stan. Univ. Hum.-Centered A.I. (Aug. 2022), https://hai.stanford.edu/sites/default/files/2022-08/HAI%20Explainer%20-%20What%20The%20CHIPS%20and%20Science%20Act%20Means%20for%20AI.pdf [https://perma.cc/LU8V-J4XQ]; U.S. Dep't of Treasury, Treasury Department Mobilizes Semiconductor Supply Chain Investment Incentives with Key CHIPS Investment Tax Credit Guidance (Mar. 21, 2023), https://home.treasury.gov/news/press-releases/jy1353.

426. *Summary of AI Provisions*, *supra* note 421, at 2.

427. *Id*.

428. *Id*. at 3.

429. Press Release, S. Democrats, Majority Leader Schumer Floor Remarks On Launching The SAFE Innovation Framework For AI And First Of Their Kind AI Insight Forums (June 22, 2023), https://www.democrats.senate.gov/newsroom/press-releases/majority-leader-schumer-floor-remarks-on-launching-the-safe-innovation-framework-for-ai-and-first-of-their-kind-ai-insight-forums; Gabby Miller, *U.S. Senate AI 'Insight Forum' Tracker*, Tech. Pol'y Press (Dec. 8, 2023), https://techpolicy.press/us-senate-ai-insight-forum-tracker/.

every congressional committee has held hearings to educate themselves on AI in their purview, from the Senate Judiciary Committee and Senate Committee on Homeland Security and Government Affairs, to the House Judiciary Subcommittee on Courts, Intellectual Property, and the Internet.[430] These efforts have been integrated with support from civil society and private industry. In addition to the highly acclaimed programs offered by Stanford Human-Centered Artificial Intelligence[431] and the Woodrow Wilson International Center[432] for Scholars, EqualAI,[433] for example, launched a bipartisan, bicameral pilot program to offer an "AI Deep Dive" workshop to Hill staff who had AI proficiency and whose Members were drafting AI legislation.[434]

There are several noteworthy attempts to establish comprehensive federal AI legislation in the U.S. One of the first AI-focused bills was the Algorithmic Accountability Act ("AAA"), first presented in 2019, which aimed to reduce inaccurate, unfair, biased, or discriminatory AI decisions impacting Americans. Building off the 2019 AAA, Senator Ron Wyden (D-OR.), Senator Cory Booker (D-NJ), and Representative Yvette Clarke (D-NY) reintroduced the AAA in 2022.[435] This bill sought to increase transparency and oversight by requiring companies to assess the impacts of automated decision-making and giving the FTC greater regulatory authority over AI systems.[436]

Generative AI has invigorated public curiosity about AI more broadly and heightened elected officials' focus on regulation.

---

430. *Hearing on Artificial Intelligence in Government, Comm. on Homeland Security & Governmental Affairs*, 118th Cong. (May 16, 2023), https://www.hsgac.senate.gov/hearings/artificial-intelligence-in-government/; *Oversight of AI: Principles for Regulation: Hearing Before the S. Comm. on the Judiciary*, 118th Cong. (2023), https://www.judiciary.senate.gov/committee-activity/hearings/oversight-of-ai-principles-for-regulation; *Artificial Intelligence and Intellectual Property: Part I: Hearing Before the H. Comm. on the Judiciary*, 118th Cong. (2023), https://judiciary.house.gov/committee-activity/hearings/artificial-intelligence-and-intellectual-property-part-i.

431. Stan. Univ. Hum.-Centered A.I., *Congressional Boot Camp on AI*, https://hai.stanford.edu/congressional-boot-camp-ai.

432. Wilson Ctr., *Artificial Intelligence Lab*, https://www.wilsoncenter.org/artificial-intelligence-lab.

433. For transparency, authors Miriam Vogel and Jim Wiley are respectively the President and CEO and Legal and Research Director of EqualAI.

434. EqualAI, *Congressional Responsible AI Policy Workshop Pilot Program*, https://www.equalai.org/programs/responsible-ai-policy-workshop/.

435. Press Release, Sen. Ron Wyden, Wyden, Booker, Clarke Introduce Bill Requiring Companies To Target Bias In Corporate Algorithms (Apr. 10, 2019), https://www.wyden.senate.gov/news/press-releases/wyden-booker-clarke-introduce-bill-requiring-companies-to-target-bias-in-corporate-algorithms-

436. Press Release, Sen. Ron Wyden, Algorithmic Accountability Act of 2022, https://www.wyden.senate.gov/imo/media/doc/2022-02-03%20Algorithmic%20Accountability%20Act%20of%202022%20One-pager.pdf.

Unsurprisingly, the number of AI legislative proposals has substantially increased, surpassing 180 last year.[437]

Soon after the release of ChatGPT, Representative Ted Lieu (D-CA) introduced a nonbinding measure written entirely by the generative AI tool, invoking the technology itself to call on the House of Representatives to scrutinize AI's increased sophistication and use.[438] In a related op-ed, Lieu shared a quote from ChatGPT that "the time to act is now to ensure that AI is used in ways that are safe, ethical and beneficial for society," and "[f]ailure to do so could lead to a future where the risks of AI far outweigh its benefits."[439]

In 2023, Senator Chuck Schumer and a bipartisan group of Senators proposed a roadmap for AI regulation with the SAFE Innovation Framework.[440] This framework intends to provide a legislative roadmap on AI and consists of five central pillars: protecting national security, achieving accountability through supporting "responsible" AI systems, requiring that AI systems align with foundational democratic values, ensuring AI systems are explainable to users, and bolstering U.S. AI innovation.

In 2024, the Bipartisan Senate AI Working Group released Driving U.S. Innovation in Artificial Intelligence as a culminating roadmap following Senate briefings and the nine AI Insight Forums sessions. This roadmap provides the findings from these educational efforts and identifies policy areas for future bipartisan efforts around AI. The roadmap is divided into eight sections reflecting the insight forum sessions: Supporting U.S. Innovation in AI; AI and the Workforce; High Impact Uses of AI; Elections and Democracy; Privacy and Liability; Transparency, Explainability, Intellectual Property, and Copyright; Safeguarding Against AI Risks; National Security.[441]

---

437. *Congressional Boot Camp on AI*, supra note 431.

438. Kate Santaliz & Julie Tsirkin, *AI wrote a bill to regulate AI. Now Rep. Ted Lieu wants Congress to pass it*, NBC News (Jan. 26, 2023), https://www.nbcnews.com/politics/congress/ted-lieu-artificial-intelligence-bill-congress-chatgpt-rcna67752.

439. Ted Lieu, *I'm a Congressman Who Codes. A.I. Freaks Me Out*, N.Y. Times (Jan. 23, 2023), https://www.nytimes.com/2023/01/23/opinion/ted-lieu-ai-chatgpt-congress.html; Santaliz, *supra* note 438.

440. Press Release, Sen. Democrats, Majority Leader Schumer Delivers Remarks To Launch SAFE Innovation Framework For Artificial Intelligence At CSIS (June 21, 2023), https://www.democrats.senate.gov/news/press-releases/majority-leader-schumer-delivers-remarks-to-launch-safe-innovation-framework-for-artificial-intelligence-at-csis.

441. The Bipartisan S. Working Grp., *Driving U.S. Innovation in Artificial Intelligence*, (May 2024), https://www.schumer.senate.gov/imo/media/doc/Roadmap_Electronic1.32pm.pdf [https://perma.cc/CE8L-BHZM].

Other examples of notable federal bipartisan legislation include[442]:

- Senators Maria Cantwell (D-WA), Todd Young (R-IN), John Hickenlooper (D-CO), and Marsha Blackburn (R-TN) proposed the Future of AI Innovation Act to promote AI research and unify standards for evaluating AI by authorizing the AI Safety Institute to develop AI standards, creating new testbeds to evaluate AI models, and accelerating AI innovation with publicly available data sets.[443]
- Senators Mitt Romney (R-UT), Jack Reed (D-RI), Jerry Moran (R-KS), and Angus King (I-ME) proposed a framework for addressing "AI-enabled extreme risks from biological, chemical, cyber, and nuclear threats."[444] The framework recommends that the federal government oversee efforts to mitigate these risks by giving oversight authority to an interagency coordinating body, an existing agency, or a new agency. This entity would vet hardware providers, institute notification and reporting requirements when developing frontier models, and oversee the evaluation and licensing of frontier models before their release.
- Senators Josh Hawley (R-MO) and Richard Blumenthal (D-CT) developed a bipartisan bill to "establish a licensing regime administered by an independent oversight body," create a private right of action and take other steps to address AI harms, limit the transfer of AI technology to geopolitical rivals, promote transparency on models and their outputs, and protect consumers and kids.[445]
- Representatives Ted Lieu (CA-36), Ken Buck (CO-4), and Anna Eshoo (CA-16) introduced bipartisan and bicameral

442. For continued updates on AI legislative proposals, see Brennan Ctr. for J., *Artificial Intelligence Legislation Tracker* (Mar. 8, 2024), https://www.brennancenter.org/our-work/research-reports/artificial-intelligence-legislation-tracker.

443. Press Release, U.S. Senate Comm. on Commerce, Sci. & Transp., Cantwell, Young, Blackburn, Hickenlooper Introduce Bill to Ensure U.S. Leads Global AI Innovation (Apr. 18, 2024), https://www.commerce.senate.gov/2024/4/cantwell-young-blackburn-hickenlooper-introduce-bill-to-ensure-u-s-leads-global-ai-innovation.

444. Press Release, Sen. Mitt Romney, Reed, Moran, King Unveil Framework to Mitigate Extreme AI Risks (Apr. 16, 2024), https://www.romney.senate.gov/romney-reed-moran-king-unveil-framework-to-mitigate-extreme-ai-risks/; Mitt Romney et al., Framework for Mitigating Extreme AI Risks, https://www.romney.senate.gov/wp-content/uploads/2024/04/AI-Framework_2pager.pdf.

445. Richard Blumenthal & Josh Hawley, Bipartisan Framework for U.S. AI Act, https://www.blumenthal.senate.gov/imo/media/doc/09072023bipartisanaiframework.pdf.

legislation[446] to create a national commission to advise Congress on regulating AI.[447]

- Senator Gary Peters (D-MI) proposed a bill to require transparency in the federal government's use of AI, including notifications to individuals, appeals, and human review of AI decisions.[448]
- Senator Michael Bennet (D-CO) introduced an act to ensure the U.S. government leads by example in the responsible use of AI by requiring a top-to-bottom review of existing AI policies across the federal government. It would also "generate specific regulatory and legislative recommendations intended to ensure that the federal government's AI tools and policies respect civil rights, civil liberties, privacy, and due process."[449]
- Senators Michael Bennet (D-CO), Todd Young (R-IN), and Mark Warner (D-VA) introduced a bipartisan bill to create an Office of Global Competition Analysis. This office would evaluate the U.S.'s standing in technologies like AI compared to other countries, aiming to inform U.S. policy and enhance American competitiveness.[450]
- Senators John Thune (R-SD) and Amy Klobuchar (D-MN) spearheaded the proposal of the Artificial Intelligence (AI) Research, Innovation, and Accountability Act of 2023 to require companies deploying generative AI to provide notice to users, require detailed risk assessments and certifications for "critical-impact" uses and direct the department of commerce to provide recommendations on promoting consumer education for AI.[451]

---

446. For forthcoming companion litigation in the Senate, see Press Release, Rep. Ted Lieu, Reps Lieu, Buck, Eshoo and Sen Schatz Introduce Bipartisan, Bicameral Bill to Create a National Commission on Artificial Intelligence (June 20, 2023), http://lieu.house.gov/media-center/press-releases/reps-lieu-buck-eshoo-and-sen-schatz-introduce-bipartisan-bicameral-bill.

447. *Id.*

448. Press Release, Sen. Gary Peters, Peters Introduces Bipartisan Bill to Require Transparency of Federal Government's Use of AI, (June 8, 2023), https://www.peters.senate.gov/newsroom/press-releases/peters-introduces-bipartisan-bill-to-require-transparency-of-federal-governments-use-of-ai.

449. Press Release, Sen. Michael Bennet, Bennet Introduces Legislation to Stand Up An AI Task Force to Ensure Responsible Use of The Technology By The Federal Government (Apr. 28, 2023), https://www.bennet.senate.gov/public/index.cfm/2023/4/bennet-introduces-legislation-to-stand-up-an-ai-task-force-to-ensure-responsible-use-of-the-technology-by-the-federal-government.

450. Press Release, Sen. Michael Bennet, Bennet, Young, Warner Introduce Bill to Strengthen U.S. Technology Competitiveness (June 8, 2023), https://www.bennet.senate.gov/public/index.cfm/2023/6/bennet-young-warner-introduce-bill-to-strengthen-u-s-technology-competitiveness.

451. Press Release, Thune, Klobuchar Lead Commerce Committee Colleagues in Introducing Bipartisan AI Bill to Boost Innovation and Strengthen Accountability

Although these bills have not become law, they reflect Congress' efforts to address AI safety use and its impact on national security, government use and overall governance. The uptick in bills, as well as their bipartisan and bicameral support, signal a strong intention to realize more regulation and oversight in AI policy than has been achieved in other areas of significant import, time and attention, such as privacy and social media policy. Each section of this Article addresses foundations of law that will govern wide swaths of AI use and deployment, and we can expect that the U.S. government will build on efforts noted in this and earlier sections to further fill gaps and establish a clear framework.

C. White House / Executive Office of the President

The U.S. federal executive branch has significantly shaped federal AI policy in recent years through executive orders and various department-specific actions which are shaping principles and standards around acceptable AI uses; developing recommendations around best practices, evaluations, and safeguards; creating government regulatory capacity; and steering private sector innovation.

1. Executive Orders and Actions

Numerous executive actions have been issued to consolidate and clarify government processes and expectations. On October 30, 2023, President Biden signed the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.[452] This sweeping executive order ("EO") sets standards for safety and security; protects privacy, equity and civil rights; encourages innovation; supports consumers and workers; and promotes U.S. leadership in responsible AI.[453] It specifically calls for federal regulatory actions, including requiring government notifications and red-teaming for highly advanced AI models, calling for the development of guidance for content authentication, strengthening privacy tools, instituting training on AI civil rights enforcement, creating resources to support educators,

(Nov. 15, 2023) https://www.thune.senate.gov/public/index.cfm/2023/11/thune-klobuchar-lead-commerce-committee-colleagues-in-introducing-bipartisan-ai-bill-to-boost-innovation-and-strengthen-accountability [https://perma.cc/34XP-22Y7].

452. Exec. Order No. 14110, 88 Fed. Reg. 75191 (Oct. 30, 2023), https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

453. Press Release, White House, FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, Press Release (Oct. 30 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/.

catalyzing AI research through a pilot of NAIRR and providing research assistance to small developers and entrepreneurs, and encouraging increased bilateral and multilateral collaboration on AI at the global scale.

This EO builds on several prior EOs, including EO 13859 on Maintaining American Leadership in AI[454] and EO 13960 on Promoting the Use of Trustworthy AI in the Federal Government.[455]. President Biden signed an executive order requiring federal agencies to remove bias in the design and use of AI technologies in February 2023.[456]

In the summer of 2023, 15 AI "frontier" companies, or those developing generative AI, including Amazon, Google, OpenAI, ScaleAI, Stability, and Microsoft, went to the White House to announce voluntary commitments to manage risks associated with AI.[457] These companies agreed to abide by 8 measures include pre-release of safety testing, industry-wide information sharing, cybersecurity investments,

454. Exec. Order No. 13859, 84 Fed. Reg. 3967 (Feb. 11, 2019), https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence. Under EO 13859, the U.S. established the first seven national AI research institutes, encouraged work on AI technical standards, provided OMB guidance for AI regulation in the private sector, and supported international alliances. *Id.*

455. Exec. Order No. 13960, 85 Fed. Reg. 78939 (Dec. 3, 2020), https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government. EO 13960 established AI principles for the federal government and policies for implementation, directed agencies to engage in AI cataloging, and encouraged the implementation of AI within federal agencies. *Id.*

456. Press Release, White House, FACT SHEET: Biden-Harris Administration Announces New Actions to Promote Responsible AI Innovation that Protects Americans' Rights and Safety (May 4, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-new-actions-to-promote-responsible-ai-innovation-that-protects-americans-rights-and-safety; Exec. Order No. 14091, 88 Fed. Reg. 10825 (Feb. 16, 2023), https://www.federalregister.gov/documents/2023/02/22/2023-03779/further-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal.

457. Press Release, White House, FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI (July 21, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/; Press Release, White House, FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Eight Additional Artificial Intelligence Companies to Manage the Risks Posed by AI (Sept. 12, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/09/12/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-eight-additional-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/.

watermarking and other transparency efforts to ensure public trust, and ongoing research into AI's societal risks and potential benefits.[458]

2. Blueprint for AI Bill of Rights

In October 2022, the Office of Science and Technology Policy ("OSTP") released a Blueprint for an AI Bill of Rights[459] as well as correlated actions across the executive branch to promote accountability and protecting rights with regard to technology use.[460] The Blueprint identifies "five principles that should guide the design, use, and deployment of automated systems to protect the American public in the age of artificial intelligence."[461] These principles[462] are safe and effective systems;[463] algorithmic discrimination protections;[464] data privacy;[465] notice and explanation;[466] and human alternatives, consideration, and fallback.[467] The Blueprint clarifies that systems fall within its purview if they are: "(1) automated systems that (2) have the potential to meaningfully impact the American public's rights, opportunities, or access to critical resources or services."[468] In accordance with these principles, Executive Order 14110, and the NIST AI RMF, the OMB published a Memorandum on Advancing Governance, Innovation, and

458. Press Release, Am. Nat'l Standards Inst., Leading AI Companies Sign U.S. Government Commitment On Safety, Security, And Trust In Ai Development (July 21, 2023), https://www.ansi.org/standards-news/all-news/2023/07/7-21-23-leading-ai-companies-sign-us-government-commitment.

459. White House Off. of Sci. & Tech. Pol'y, *Blueprint for an AI Bill of Rights*, https://www.whitehouse.gov/ostp/ai-bill-of-rights/ [https://perma.cc/CF42-TNK9] (last visited Aug. 8, 2024).

460. Press Release, White House, FACT SHEET: Biden-Harris Administration Announces Key Actions to Advance Tech Accountability and Protect the Rights of the American Public (Oct. 4, 2023), https://www.whitehouse.gov/ostp/news-updates/2022/10/04/fact-sheet-biden-harris-administration-announces-key-actions-to-advance-tech-accountability-and-protect-the-rights-of-the-american-public/.

461. *Blueprint for an AI Bill of Rights*, *supra* note 459.

462. *Id.*

463. *Blueprint for an AI Bill of Rights*, *supra* note 459.

464. White House Off. of Sci. & Tech. Pol'y, *Algorithmic Discrimination Protections*, https://www.whitehouse.gov/ostp/ai-bill-of-rights/algorithmic-discrimination-protections-2/ [https://perma.cc/LR3F-EVJE] (last visited Aug. 8, 2024).

465. White House Off. of Sci. & Tech. Pol'y, *Data Privacy*, https://www.whitehouse.gov/ostp/ai-bill-of-rights/data-privacy-2/ [https://perma.cc/HQ5K-QLF6] (last visited Aug. 8, 2024).

466. White House Off. of Sci. & Tech. Pol'y, *Notice and Explanation*, https://www.whitehouse.gov/ostp/ai-bill-of-rights/notice-and-explanation/ [https://perma.cc/97WZ-D9EN] (last visited Aug. 8, 2024).

467. White House Off. of Sci. & Tech. Pol'y, Human Alternatives, Consideration, and Fallback, https://www.whitehouse.gov/ostp/ai-bill-of-rights/human-alternatives-consideration-and-fallback/ [https://perma.cc/A9TA-H8TX] (last visited Aug. 8, 2024).

468. *Blueprint for an AI Bill of Rights*, *supra* note 459.

Risk Management for Agency Use of Artificial Intelligence in March 2024,[469] which focuses on AI governance, advancing responsible innovation, and managing risks from the use of AI.

3. NAIIO and NAIAC

The National Artificial Intelligence Initiative Office ("NAIIO") and National AI Advisory Committee ("NAIAC") are two entities that support the White House in the coordination of AI initiatives and policies. NAIIO is based at the White House Office of Science and Technology Policy ("OSTP") and is tasked with providing technical and administrative support to the interagency coordination of AI efforts and working on public initiatives and outreach.[470] NAIAC is an interdisciplinary group of AI experts and leaders appointed by the president to provide the White House with recommendations on AI policy in areas including research and development, international collaboration, workforce, and competitiveness.[471] Additionally, numerous internal working groups and task forces, including the Artificial Intelligence Research and Development Interagency Working Group ("AI R&D IWG"), have been formed to coordinate efforts across federal agencies.[472]

D. Commerce Department

A significant development in AI policy came from a small division within the U.S. Commerce Department in early 2023. The National Institute for Standards and Technology ("NIST") released an AI Risk Management Framework ("AI RMF"),[473] as congressionally mandated in NDAA 2021.[474] In order to facilitate and navigate use of the AI RMF, NIST released an accompanying guide, the draft AI RMF Playbook ("Playbook") on January 26, 2023.[475] The AI RMF aims to

469. Office of Mgmt. & Budget, Exec. Off. of the President, Memorandum No. M-24-10, Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence (Mar. 2024), https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf.

470. WHITE HOUSE OFF. OF SCI. & TECH. POL'Y, *Technology*, https://www.whitehouse.gov/ostp/ostps-teams/technology/.

471. AI.GOV, *National AI Advisory Committee* (last visited May 27, 2024), https://www.ai.gov/naiac [https://perma.cc/L2VN-7PMG].

472. NITRD, *Artificial Intelligence R&D Interagency Working Group*, https://www.nitrd.gov/coordination-areas/ai/ (last visited Mar. 25, 2024).

473. AI RMF 1.0, *supra* note 17.

474. National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 3388, https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf.

475. AI RMF 1.0, *supra* note 17.

help organizations manage individuals', organizations', and societal risks that are associated with AI. It is intended for voluntary use and to improve organizations' incorporation of trustworthiness considerations into their AI products, services, and systems. This document has been lauded as an invaluable tool to guide organizations on best practices in reducing harms from AI.[476] EqualAI produced an AI Impact Assessment tool ("AIA") based on the NIST RMF to help increase awareness and adoption of these best practices by all organizations that use AI systems in pivotal functions.[477] In addition to the AI RMF, NIST released guidance on generative AI risks,[478] software development practices,[479] reducing risks of synthetic content,[480] and a plan for global AI standards.[481] NIST also launched NIST GenAI, a program which aims to evaluate generative AI technologies.[482]

The recently launched U.S. AI Safety Institute ("AISI"), housed within NIST (established in February 2024), was created to advance the study and science around AI safety, with a specific focus on risks involving national security, public safety, and individual rights.[483] The AISI intends to support research around AI measurement and evaluation, developing guidelines for risk mitigation.[484] To support its efforts, the AISI Consortium (AISIC) was established to include

476. Nat'l Inst. of Standards & Tech., *Perspectives about the NIST Artificial Intelligence Risk Management Framework* (Sept. 14, 2023), https://www.nist.gov/itl/ai-risk-management-framework/perspectives-about-nist-artificial-intelligence-risk-management.

477. EqualAI, *EqualAI Algorithmic Impact Assessment (AIA)*, https://www.equalai.org/aia/.

478. Nat'l Instit. of Standards & Tech., NIST AI 600-1, Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (2024), https://airc.nist.gov/docs/NIST.AI.600-1.GenAI-Profile.ipd.pdf [https://perma.cc/F9X8-GBZN].

479. Nat'l Inst. of Standards & Tech., NIST SP 800-218A i, Secure Software Development Practices for Generative AI and Dual-Use Foundation Models (2024), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218A.ipd.pdf [https://perma.cc/R26T-BAEF].

480. Nat'l Inst. of Standards & Tech., NIST AI 100-4, Reducing Risks Posed by Synthetic Content (2024), https://airc.nist.gov/docs/NIST.AI.100-4.SyntheticContent.ipd.pdf [https://perma.cc/P7FB-YL4Y].

481. Nat'l Inst. of Standards & Tech., NIST AI 100-5, A Plan for Global Engagement on AI Standards (2024), https://airc.nist.gov/docs/NIST.AI.100-5.Global-Plan.ipd.pdf [https://perma.cc/KDB8-T66H].

482. *GenAI: Evaluating Generative AI Technologies*, Nat'l Inst. of Standards & Tech., https://ai-challenges.nist.gov/genai [https://perma.cc/54GT-EBUQ] (last visited June 8, 2024).

483. *U.S. Artificial Intelligence Safety Institute*, Nat'l Inst. of Standards & Tech., https://www.nist.gov/aisi [https://perma.cc/EA9J-LLXW] (last visited June 8, 2024).

484. *Id.*

additional non-government stakeholders. The group holds more than 200 member companies, including creators, users, scholars, researchers, and organizations that promote civil society.[485] In July 2024, the AISI released its first guidance for public comment, identifying best practices for measuring risks and steps to prevent these models from assisting malicious activity.[486]

Through these and other divisions, including the National Telecommunications and Information Administration ("NTIA"), the Patent and Trademark Office ("PTO") and the Bureau of Industry and Security ("BIS"), the Department of Commerce will direct policy and practice around AI safety and provide resources to organizations and savvy AI users and their lawyers will continue to monitor these Commerce divisions' developments to learn best practices and potential restrictions or liabilities.

E. State Department

On February 16, 2023, the State Department released a set of guidelines for States across the globe incorporating AI into defense operations.[487] These global guidelines are not legally enforceable, but they were presented at the international Summit on Responsible AI in the Military Domain and are intended to serve as a foundation for international collaboration on the governance of AI systems in the military.[488] Of note, it directs human involvement in a tech-enhanced military system, especially in overseeing sensitive operations, in order to reduce bias and accidents.[489] Additional AI initiatives at the Department of State stem from numerous offices and bureaus, including

485. *Biden-Harris Administration Announces First-Ever Consortium Dedicated to AI Safety*, Nat'l Inst. of Standards & Tech., https://www.nist.gov/news-events/news/2024/02/biden-harris-administration-announces-first-ever-consortium-dedicated-ai [https://perma.cc/Q9XK-YSKG] (last visited June 8, 2024).

486. *Department of Commerce Announces New Guidance, Tools 270 Days Following President Biden's Executive Order on AI*, Nat'l Inst. of Standards & Tech. (July 26, 2024), https://www.nist.gov/news-events/news/2024/07/department-commerce-announces-new-guidance-tools-270-days-following.

487. U.S. Dep't of State, Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy (last visited May 27, 2024), https://www.state.gov/wp-content/uploads/2023/10/Latest-Version-Political-Declaration-on-Responsible-Military-Use-of-AI-and-Autonomy.pdf.

488. Media Note, U.S. Dep't of State, Off. of the Spokesperson, Building Consensus on the U.S. Framework for a Political Declaration on the Responsible Military Use of Artificial Intelligence and Autonomy (Feb. 16, 2023), https://www.state.gov/building-consensus-on-the-u-s-framework-for-a-political-declaration-on-the-responsible-military-use-of-artificial-intelligence-and-autonomy.

489. U.S. Dep't of State, Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, https://www.state.gov/wp-content/

the Global Engagement Center, which focuses on foreign propaganda and disinformation; the Technology Engagement Team; and the Office of the Under Secretary of State for Arms Control and International Security.[490]

Through international diplomacy, the State Department is developing consensus around AI standards, best practices, and policies, providing guidance on what AI policy and law will look like in the future and laying the foundation for developing interoperable regulatory frameworks. By understanding these policy developments and trends around standards and best practices, lawyers can understand how AI may be regulated in the future across jurisdictions.

F. Department of Defense ("DOD") / Department of Homeland Security ("DHS")

AI innovations have impacted military operations, from image recognition technology to "optimiz[ing] everything," including equipment maintenance and budgetary decisions.[491] In 2020, a human operator lost to an AI-operated F-16 in a simulated dogfight.[492] In December 2022, DOD successfully flew an AI-piloted F-16.[493]

DOD adopted ethical principles in 2020[494] and detailed its plan for operationalization of those principles two years later in the *Responsible AI (RAI) Strategy and Implementation (S&I) Pathway*, which emphasized the need to "maintain our military advantage in a

uploads/2023/10/Latest-Version-Political-Declaration-on-Responsible-Military-Use-of-AI-and-Autonomy.pdf (last visited May 27, 2024).

490. *Artificial Intelligence (AI)*, U.S. DEP'T OF STATE, https://www.state.gov/artificial-intelligence [https://perma.cc/GNB5-BLYQ] (last visited May 27, 2024).

491. Michèle A. Flournoy, *AI Is Already at War*, FOREIGN AFFS. (Oct. 24, 2023), https://www.foreignaffairs.com/united-states/ai-already-war-flournoy.

492. Ryan Pickrell, *A US Air Force F-16 pilot just battled AI in 5 simulated dogfights, and the machine emerged victorious every time*, BUS. INSIDER (Aug. 21, 2020, 3:59 PM), https://www.businessinsider.com/ai-just-beat-a-human-pilot-in-a-simulated-dogfight-2020-8.

493. Tom Ward, *The US Air Force Is Moving Fast on AI-Piloted Fighter Jets*, WIRED (Mar. 8, 2023, 10:52 AM), https://www.wired.com/story/us-air-force-skyborg-vista-ai-fighter-jets.

494. Release, U.S. Dep't of Defense, DOD Adopts Ethical Principles for Artificial Intelligence (Feb. 24, 2020), https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence.

digitally competitive world."[495] The DOD consulted those principles when updating its "Autonomy in Weapon Systems" directive in 2023.[496]

DOD has created entirely new positions and offices to address AI threats and use, including the establishment of a Chief Digital and Artificial Intelligence Office, an Emerging Capabilities Policy Office, a Defense Innovation Unit, and an Office of Strategic Capital to better integrate technology into its work.[497]

Several members of Congress have introduced bills focused on AI safety in the military context. For example, Representatives Ken Buck, Ted Lieu, and Don Beyer, and Senator Ed Markey, introduced bipartisan and bicameral legislation "to safeguard the nuclear command and control process from any policy that allows AI to make nuclear launch determinations."[498] Representatives Anna Eshoo, Michael McCaul, Don Beyer, and Jay Obernolte introduced bipartisan legislation to establish "the National Artificial Intelligence Research Resource ("NAIRR") as a shared national research infrastructure that provides AI researchers and students from diverse backgrounds with greater access to the complex resources, data, and tools needed to develop safe and trustworthy AI."[499]

The Department of Homeland Security ("DHS") has utilized AI to conduct operations from border security, to disaster relief efforts, to cyber threats, and child exploitation.[500] For instance, in 2023 US Customers and Border Control ("CBP") was alerted to a car's suspicious driving pattern at the U.S.-Mexico border which led to arrest of the driver trafficking 75 kilograms of narcotics. And in August of 2023, through

---

495. U.S. Dep't of Defense, Responsible Artificial Intelligence Strategy and Implementation Pathway (June 2022), https://www.ai.mil/docs/RAI_Strategy_and_Implementation_Pathway_6-21-22.pdf.

496. U.S. Dep't of Defense, Autonomy in Weapon Systems, Directive 3000.09 (Jan. 25, 2023).

497. Edward Graham, *DOD Official: AI and Autonomy Are Critical to the Future of War*, NextGov (Feb. 23, 2023), https://www.nextgov.com/artificial-intelligence/2023/02/dod-official-ai-and-autonomy-are-critical-future-war/383263.

498. Press Release, Rep. Ken Buck, Buck, Beyer, Markey, and Lieu Introduce Bipartisan Legislation to Prevent AI From Launching a Nuclear Weapon (Apr. 26, 2023), https://web.archive.org/web/20240313021858/https://buck.house.gov/media-center/press-releases/buck-beyer-markey-and-lieu-introduce-bipartisan-legislation-prevent-ai.

499. Press Release, Sen. Cory Booker, Booker, Heinrich, Young, Rounds Introduce Bipartisan, Bicameral Bill to Expand Access to Artificial Intelligence Research (July 28, 2023), https://www.booker.senate.gov/news/press/booker-heinrich-young-rounds-introduce-bipartisan-bicameral-bill-to-expand-access-to-artificial-intelligence-research [https://perma.cc/DD9W-P5FQ].

500. Using AI to Secure the Homeland, https://www.dhs.gov/ai/using-ai-to-secure-the-homeland [https://perma.cc/UT9Q-D83A] (last visited Aug. 7, 2024).

the use of AI, DHS identified over 300 victims of sexual exploitation resulting in the rescue of victims and arrest of perpetrators.[501]

In March 2024, DHS published its AI Roadmap outlining the agency's approach to AI adoption and initiatives across the agency. The roadmap outlines the agency's three main lines of effort: harness AI responsibly to promote DHS missions and protect individual rights, shepherd AI safety and security across the nation, and foster strong partnerships to establish AI leadership.[502]

DHS also established an Artificial Intelligence Safety and Security Board comprised of stakeholders across the private and public sectors to advise the Secretary and develop recommendations to critical infrastructure stakeholders on how to responsibly harness AI technology as well as how to safeguard against and respond to AI threats.[503]

G. State and Local Governments

Increasingly, state and local governments across the U.S. are enacting AI regulations. In 2022, at least 17 states proposed measures that would have an impact on the general use of AI.[504] This includes 60 AI-related bills, 21 of which passed.[505] Additionally, states such as Colorado, Illinois, and Vermont have created task forces or commissions to study AI.[506] This past year included a marked increase in AI activity in

501. Artificial Intelligence at DHS, https://www.dhs.gov/ai (last visited Aug. 7, 2024).

502. Artificial Intelligence Roadmap 2024, https://www.dhs.gov/sites/default/files/2024-03/24_0315_ocio_roadmap_artificialintelligence-ciov3-signed-508.pdf

503. Press Release, Over 20 Technology and Critical Infrastructure Executives, Civil Rights Leaders, Academics, and Policymakers Join New DHS Artificial Intelligence Safety and Security Board to Advance AI's Responsible Development and Deployment (Apr. 26 2024), https://www.dhs.gov/news/2024/04/26/over-20-technology-and-critical-infrastructure-executives-civil-rights-leaders

504. *See* Nat'l Conf. of State Legislatures, Legislation Related to Artificial Intelligence (Jan. 31 2023), https://www.ncsl.org/technology-and-communication/legislation-related-to-artificial-intelligence (providing an updated report as of January 31, 2023, on legislation related to Artificial Intelligence across the U.S.).

505. Maslej et al., *supra* note 91.

506. Nat'l Conf. of State Legislatures, Legislation Related to Artificial Intelligence (Jan. 31, 2023), https://www.ncsl.org/technology-and-communication/legislation-related-to-artificial-intelligence.

state legislatures, with 30 states and the District of Columbia[507]proposing measures and 14 AI-related laws enacted across 9 states.[508]

The U.S. government has made foundational investments across government to bolster the country's AI readiness and ensure leadership in AI research and development. The State Department's engagement in international fora like the UK Summit on Responsible AI[509] and the Trade and Technology Council ("TTC")[510] demonstrate a commitment to fostering global collaboration in AI governance. Within DOD, the adoption of ethical principles and the development of the Responsible AI Strategy and Implementation Pathway reflect a proactive approach to integrating AI while balancing military advantage and ethical considerations. Pending legislative proposals further underscore the ongoing U.S. government focus on the use of—and limits on the use of-- AI in critical domains, such as nuclear command and control, while also promoting access to AI research resources for researchers and more diverse stakeholders.

VII. Global Perspectives on AI

AI technologies cross geographical and political borders in nearly all of its applications. As such, when building or using an AI system, it is important for developers and their legal teams to consider legal frameworks and international agreements developed by various countries and international organizations.[511] This section outlines

507. Press Release, Off. of the Att'y Gen. for D.C., AG Racine Introduces Legislation to Stop Discrimination In Automated Decision-Making Tools That Impact Individuals' Daily Lives (Dec. 9, 2021), https://oag.dc.gov/release/ag-racine-introduces-legislation-stop.

508. Margaret Harding McGill, *AI Legislation Picks up Steam in Congress, States*, Axios (Sept. 28, 2023), https://www.axios.com/2023/09/28/ai-legislation-congress-states.

509. AI SAFETY SUMMIT, https://www.aisafetysummit.gov.uk (last visited July 9, 2024).

510. Office of the United States Trade Representative, *U.S.-E.U. TRADE AND TECHNOLOGY COUNCIL (TTC)* [hereinafter *TTC*], https://ustr.gov/useuttc [https://perma.cc/8B5T-39UN] (last visited July 9, 2024).

511. The U.S. has participated in several international agreements, including the OECD Principles on AI, adopted by forty-two countries in 2019, and the 2021 Recommendation on the Ethics of Artificial Intelligence, adopted by 193 countries. *OECD AI Principles Overview*, *supra* note 14; *UNESCO adopts first global standard on the ethics of artificial intelligence*, UNESCO (Apr. 8, 2022), https://www.unesco.org/en/articles/unesco-adopts-first-global-standard-ethics-artificial-intelligence. The U.S. has also participated in international coalitions such as the Global Partnership on AI (GPAI). GPAI, https://www.gpai.ai/about/ (last visited July 9, 2024). Although the U.S. has diverged from the EU in some respects on how it regulates AI, it has made bilateral and multilateral efforts to find common ground with the EU and other global entities. Alex Engler, *The EU and U.S. diverge on AI regulation: A transatlantic comparison and steps to alignment*, Brookings (Apr. 25, 2023), https://

ongoing developments in international AI regulations and data privacy laws and focuses on several key jurisdictions, including the European Union ("EU"), Brazil, Canada, China, Japan, Singapore, and the United Kingdom.

As reported by the OECD, over 1,000 policy initiatives enacted by more than 70 countries, territories, and the EU govern the development or use of AI.[512] These initiatives influence how countries set business and legal standards and cooperate in the creation and regulation of AI.[513] Across the globe, data privacy laws have become increasingly prevalent, with nearly 140 countries passing some form of legislation to protect the data and privacy of their citizenry.[514] As discussed below, the significance of data in AI systems underscores the pivotal role of data privacy laws that will continue to shape AI regulation.

The following discussion offers examples of prominent international regulatory proposals and approaches that are shaping the AI legal landscape.

A. European Union

The EU has led in the global AI policy arena with the recently released Artificial Intelligence Act.[515] This framework is intended to regulate AI systems in the EU market and beyond, and it introduces rules ensuring the and trustworthiness of AI systems. Similar to the EU's General Data Protection Regulation, the AI Act is expected to have a global "Brussels effect,"[516] impacting foreign providers and

---

www.brookings.edu/articles/the-eu-and-us-diverge-on-ai-regulation-a-transatlantic-comparison-and-steps-to-alignment/; *see, e.g.*, *TTC*, *supra* note 510; U.S. – India Artificial Intelligence (USIAI) INitiative, https://usiai.iusstf.org (last visited July 9, 2024); Press Release, U.S. Nat'l Scis. Found., New NSF-Australia awards will tackle responsible and ethical artificial intelligence (Feb. 19, 2023), https://new.nsf.gov/news/new-nsf-australia-awards-will-tackle-responsible.

512. OECD, *National AI policies & strategies*, https://oecd.ai/en/dashboards/overview (last visited Mar. 24, 2024).

513. *See generally id.*; *see also* Elham Tabassi et al., OECD, *National AI policies & strategies* (Dec. 20, 2023), https://oecd.ai/en/wonk/united-states-ai-for-all-policy.

514. UNCTAD, *Data Protection and Privacy Legislation Worldwide* https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (last visited Mar. 24, 2024).

515. Eur. Parl., *EU AI Act: first regulation on artificial intelligence* (Dec. 19, 2023) [hereinafter *EU AI Act*], https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence;https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf.

516. *See* Anu Bradford, *The Brussels Effect*, 107 Nw. U. L. Rev. 1 (2012), https://scholarship.law.columbia.edu/faculty_scholarship/271 (discussing the principle that, through first-mover regulations, the EU is shaping international business and regulatory policy).

users that operate within the EU.[517] This extraterritorial impact demands familiarity with the nuances of the regulation, as breaches can lead to 35 million euros or 7 percent of a company's total annual turnover in the prior year, whichever is larger.[518]

The EU AI Act regulates companies using AI through a risk-based, legal framework—i.e., applying to all applications across sectors—that separates AI use into four categories of risk: unacceptable, high, limited, and minimal or no risk.[519] The level of risk dictates the amount of regulation that will apply. For example, domains where AI risk is deemed unacceptable are completely banned, such as social scoring by governments.[520] Minimal to no risk systems are not subject to regulation. These might include AI-enabled video games or spam filters. Limited risk systems, such as chatbots, must meet certain transparency requirements. High risk systems, such as employment, law enforcement, education, or critical infrastructure, are "subject to strict obligations," according to the European Commission, "before they can be put on the market."[521]

In June 2023, EU lawmakers adopted a version of the Act that incorporated requirements for generative AI models.[522] These included disclosing when content is AI-generated, imposing safeguards against the generation of illegal content, and making public any summaries of copyrighted data that was used for training. In December 2023, the EU Parliament struck a deal on the Act, which included safeguards on general-purpose AI, restrictions on biometric AI, bans on social scoring and certain exploitative behaviors, and consumer rights to explanations

517. Alex Engler, *The EU AI Act will have global impact, but a limited Brussels Effect*, Brookings (June 8, 2022), https://www.brookings.edu/research/the-eu-ai-act-will-have-global-impact-but-a-limited-brussels-effect/.

518. Press Release, Eur. Parl., Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI, (Dec. 9, 2023), https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai.

519. Eur. Comm'n, *AI Act*, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (last visited Mar. 24, 2024).

520. *Id.*

521. *Id.*

522. Ryan Browne, *EU lawmakers pass landmark artificial intelligence regulation*, CNBC (June 14, 2023), https://www.cnbc.com/2023/06/14/eu-lawmakers-pass-landmark-artificial-intelligence-regulation.html; Eur. Parl., *EU AI Act: first regulation on artificial intelligence* (Dec. 19, 2023), https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence; Press Release, Eur. Parl., MEPs ready to negotiate first-ever rules for safe and transparent AI (June 14, 2023), https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai.

and lodging complaints.[523] The Act was adopted by the Members of European Parliament in March 2024 and went into force on August 1, 2024.[524]

In 2018, the EU passed the General Data Protection Regulation ("GDPR"),[525] a comprehensive regulation governing the protection and use of personal data. An EU Parliament study concluded that "[d]ata protection is at the forefront of the relationship between AI and the law, as many AI applications involve the massive processing of personal data."[526] As a result, "data protection has been the area of the law that has most engaged with AI."[527]

In May 2023, the National Artificial Intelligence Advisory Committee ("NAIAC") noted in its first-year report to the President, "Article 22 [of the GDPR] has become known as the right against solely automated decisions and also the right to meaningful information about automated processes."[528] Article 22 sets forth a person's "right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects."[529] Failing to adhere to the mandates of Article 22 can expose companies to significant liability.

In an April 2022 report examining the enforcement of GDPR on automated decision-making, the Future of Privacy Forum identified more than "70 cases—19 court rulings and more than 50 enforcement decisions, individual opinions or general guidance issued by DPAs[sic]—from a span of 18 EEA Member-States, the UK and the European Data Protection Supervisor (EDPS)."[530] The report found

523. *EU AI Act*, *supra* note 515.

524. Press Release, Artificial Intelligence Act: MEPs adopt landmark law (Mar. 13, 2024), https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law; Press Release, European Artificial Intelligence Act comes into force (Aug. 1 2024), https://ec.europa.eu/commission/presscorner/detail/en/IP_24_4123.

525. 2016 J.O. (L.119) 1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

526. Giovanni Sartor, Eur. Parl. Study, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence (June 2020), https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.

527. *Id.*

528. Nat'l. A.I. Advisory Comm., National Artificial Intelligence Advisory Committee Year 1 Report (May 2023), https://ai.gov/wp-content/uploads/2023/05/NAIAC-Report-Year1.pdf.

529. 2016 J.O. (L.119) 1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

530. Sebastião Barros Vale & Gabriela Zanfir-Fortuna, Future Priv. F., Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities (2022), https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf.

that cases have begun to increase as "automated decision-making is becoming ubiquitous in daily life, and it now looks like individuals are increasingly interested in having their right under Article 22 applied."[531]

An example from 2021 involved a fine of $3 million levied on Foodinho, an on-demand food delivery company.[532] An investigation by Italy's Data Protection Authority identified a number of concerns, including that Foodihno failed to comply with Article 22's requirement to provide its riders with information on specific automated decisions and the opportunity to object to and/or request human review of these decisions.

In another case, an Amsterdam court found that even if a company, in this case Uber, did not "fully automate" its decision to terminate its driver' contracts, it could still be liable for its partially automated decisions to terminate employees for fraudulent acts.[533] The court found that the drivers had a right to access their personal data "insofar as they formed the basis for the decision to deactivate their accounts" so that the drivers could "verify the accuracy and lawfulness of the processing of their personal data."[534] Even in partially automated decisions, therefore, "drivers have the right to obtain access to their data underlying a decision to terminate their accounts" in accordance with specific GDPR transparency requirements for qualifying automated decision-making.[535]

The 39 cases summarized by the report illustrate Article 22's application to automated decision-making. However, the EU AI Act has the potential to surpass GDPR as a leading legal framework regulating AI in the world.[536] As Europe leads in implementing far-reaching tech

---

531. *Id.*

532. Natasha Lomas, *Italy's DPA fines Glovo-owned Foodinho $3M, orders changes to algorithmic management of riders*, Tech Crunch (July 6, 2021), https://techcrunch.com/2021/07/06/italys-dpa-fines-glovo-owned-foodinho-3m-orders-changes-to-algorithmic-management-of-riders/.

533. Ktr. 11, mar. 2021, ECLI 2021, 1018 (applicant/ Uber) (Neth.), https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2021:1018; *see* Vale & Zanfir-Fortuna, *supra* note 530.

534. Ktr. 11, mar. 2021, ECLI 2021, 1018 (applicant/ Uber) (Neth.), https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2021:1018 (citing Article 15 of the GDPR); *see* Council Regulation No. 2016/679, art. 15, O.J. (L 119), 43, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [https://perma.cc/R8SB-9RBH]; *see also* Vale & Zanfir-Fortuna, *supra* note 530.

535. Vale & Zanfir-Fortuna, *supra* note 530.

536. *See Shaping Europe's digital future*, EURO. COMM'N, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai#:~:text=The%20AI%20Act%20is%20the,regarding%20specific%20uses%20of%20AI [https://perma.cc/JC65-JB36] (last visited July 9, 2024) ("The AI Act is the first-ever legal framework

regulations, lawyers with transnational clients and global companies must understand their implications.

B. Brazil

Brazil's approach to AI regulation combines the EU's risk-based approach with a rights-based approach: individuals retain rights regardless of the risks. A Brazilian Senate working group submitted a report in December 2022 which contained a draft law centered around citizens' rights, categorization of risks, and sanctions.[537] It also includes rules for "(i) civil liability; (ii) codes of best practices; (iii) notification of AI incidents; (iv) administrative sanctions; (v) fostering of innovation by promoting regulatory sandboxes and creating copyright exceptions for data mining processes; and (vi) the creation of an open public database of high-risk AI systems to be held by the AI supervisory authority which contains public documents on AIA, while respecting trade secrets."[538]

The proposed bill requires that AI development and deployment follow established principles in the country's current laws, including good faith; "self-determination and freedom of choice; transparency, explainability, intelligibility, traceability, and auditability; human participation in and supervision of the AI life cycle; nondiscrimination, justice, equity, and inclusion; legal process, contestability, and compensatory damages; reliability and robustness of AI and information security; and proportionality/efficacy when using AI."[539] The bill further proposes that risk assessments be conducted and documented prior to bringing an AI system to market.[540]

Under the proposal, certain AI systems would be prohibited, including those that use subliminal techniques or exploit groups' vulnerabilities with the goal or effect of inflicting harm.[541] Public

---

on AI, which addresses the risks of AI and positions Europe to play a leading role globally.").

537. The Brazilian Report, *AI Regulation Still Lagging In Brazil*, WILSON CTR. (Mar. 23, 2023), https://www.wilsoncenter.org/blog-post/ai-regulation-still-lagging-brazil [https://perma.cc/TKV5-QR8A].

538. Cristina Akemi Shimoda Uechi & Thiago Guimarães Moraes, *Brazil's path to responsible AI*, OECD (July 27, 2023), https://oecd.ai/en/wonk/brazils-path-to-responsible-ai [https://perma.cc/L5FS-C9RQ].

539. Anna Oberschelp de Meneses et al., *Brazil's Senate Committee Publishes AI Report and Draft AI Law*, COVINGTON (Jan. 27, 2023), https://www.insideprivacy.com/emerging-technologies/brazils-senate-committee-publishes-ai-report-and-draft-ai-law/.

540. *Id.*

541. *Id.*

systems that engage in social scoring or biometric identification would also be prohibited, with narrow legal or court-authorized exceptions.[542]

The draft law would grant persons affected by AI systems certain rights regardless of the risk classification of the AI system, a provision that has generated criticism for being overly burdensome.[543] Nonetheless, the bill would establish the following rights for persons affected by any AI system: the rights to information about AI systems, to an explanation about a decision or prediction made by an AI system, to challenge those decisions or predictions, to human intervention in decisions made by AI systems, to nondiscrimination and the correction of discriminatory bias, and to privacy and the protection of personal data.[544] The bill establishes civil liability for the harms caused by the AI system, including strict liability for high-risk systems, and sets up an enforcement body that could impose a penalty up to 50 million reais (approximately $10 million) or 2 percent of a company's turnover.[545]

C. Canada

Canada introduced its own approach to an AI regulatory framework. The Artificial Intelligence and Data Act ("AIDA"), a risk-based approach to AI,[546] builds on Canada's existing consumer protection and human rights law.[547] It prohibits reckless and bad-faith uses of AI that cause significant harm and empowers enforcement by the Minister of Innovation, Science, and Industry.[548]

Although AIDA's framework is designed to stay interoperable with international AI regulation, it has a slightly different structure from the EU's approach described above.[549] Rather than banning certain high-risk uses, it would "require that appropriate measures be put in place to identify, assess, and mitigate risks of harm or biased output prior

542. *Id.*
543. Luca Belli et al., *AI Regulation In Brazil: Advancements, Flows, And Need To Learn From The Data Protection Experience*, COMPUT., L. & SEC. REV. (forthcoming) (preprint at 22), https://cyberbrics.info/ai-regulation-in-brazil-advancements-flows-and-need-to-learn-from-the-data-protection-experience/.
544. Meneses et al., *supra* note 539.
545. *Id.*
546. Jordan Shapiro & Jillian Cota, *An Overview Of Global Ai Regulation And What's Next*, PPI BLOG (Mar. 8, 2023), https://www.progressivepolicy.org/blogs/an-overview-and-of-global-ai-regulation-and-whats-next/. Unlike the EU AI Act, AIDA does not impose an outright ban on any AI tools.
547. THE ARTIFICIAL INTELLIGENCE AND DATA ACT (AIDA) – COMPANION DOCUMENT (Can.) (Mar. 13, 2023), https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document.
548. *Id*.
549. *Id*.

to a high-impact system being made.[550] The requirements for high-risk systems are guided by principles that include safety, fairness and equity, human oversight and monitoring, transparency, accountability, validity, and robustness.[551]

This legislation focuses on two types of harms—individual and systemic bias—and warns businesses which design, make available, and manage operations of AI systems that pose a high risk will be "held accountable for the creation and enforcement of appropriate internal governance processes and policies to achieve compliance with the AIDA."[552]

Canada is also proposing to update its data privacy protections. Bill C-27, the Digital Charter Implementation Act, recently passed its second reading in the House of Commons of Canada.[553] The multi-part bill would be an overhaul of Canada's privacy law and includes the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act, and the Artificial Intelligence and Data Act.[554] Following the royal assent of Bill C-27, the Canadian government would work with industry, academia, and others to guide the implementation of the law.[555] This would include determining which AI systems involve significant risk, setting standards and priorities, defining the scope and role of the AI and data commissioner, and establishing an AI advisory committee.[556]

Canada's privacy protections currently consist of several federal and provincial privacy statutes.[557] Key laws include the federal Personal Information Protection and Electronic Documents Act ("PIPEDA");[558] British Columbia's Personal Information Protection Act ("BC PIPA");[559] Alberta's Personal Information Protection Act ("AB PIPA");[560] and

550. *Id*.
551. *Id*.
552. *Id*.
553. IAPP, *Canada's Bill C-27 passes second reading* (Apr. 27, 2023), https://iapp.org/news/a/canadas-bill-c-27-passes-second-reading/.
554. *Id.* For more on the Artificial Intelligence and Data Act, see Global AI Frameworks section below.
555. *Id*.
556. *Id*.
557. Alex Cameron & Daanish Samadmoten, One Tr. Data Guidance, Canada - Data Protection Overview, https://www.dataguidance.com/notes/canada-data-protection-overview (last visited Mar. 24, 2024).
558. Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5 (Can.), https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf.
559. Personal Information Protection Act, S.B.C. 2003, c 63 (Can. B.C.), https://platform.dataguidance.com/legal-research/personal-information-protection-act-sbc-2003-c-63.
560. Personal Information Protection Act, S.A. 2003, c P-6.5 (Can. Alta.), https://kings-printer.alberta.ca/documents/Acts/P06P5.pdf.

Quebec's Act Respecting the Protection of Personal Information in the Private Sector Act ("Quebec Private Sector Act"),[561] recently amended.[562]

The federal statute, PIPEDA, is rooted in principles such as accountability, accuracy, and the ability to challenge an organization's compliance.[563] The law applies to private-sector organizations if they engage in collection, usage, or disclosure of personal information while undertaking commercial activity. It requires organizations to follow fair information principles.[564]

The privacy regulators in Canada have recently demonstrated their interest in enforcing privacy norms and regulations with regard to use of data in AI systems. The Office of the Privacy Commissioner of Canada ("OPC"), the Office of the Information and Privacy Commissioner for British Columbia, the Commission d'accès à l'information du Québec, and the Office of the Information and Privacy Commissioner of Alberta announced they will investigate OpenAI over allegations of the company's "collection, use, and disclosure of personal information without consent."[565] While details of the investigation were not disclosed, the announcement serves as a warning to other AI companies and companies that deploy AI systems that Canadian data privacy regulators intend to apply their enforcement authority to AI.

As evidenced by the EU and Canadian privacy regimes, global privacy regulators are taking note of AI and marshaling regulatory resources to ensure that companies do not violate their citizens' data privacy rights.

D. China

China has been an early mover in AI regulation. In 2017, China released its New Generation Artificial Intelligence Development Plan

561. Act Respecting the Protection of Personal Information in the Private Sector, C.Q.L.R. c P-39.1 (Can. Que.), https://www.legisquebec.gouv.qc.ca/en/pdf/cs/P-39.1.pdf.

562. Bill 64: An Act to Modernize Legislative Provisions as Regards the Protection of Personal Information, S.Q. 2021, c 25 (Can. Que.), https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/en/2021/2021C25A.PDF.

563. *PIPEDA requirements in brief*, Off. of the Priv. Comm'r of Can. (May 4, 2024), https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/.

564. *Id.*

565. News Release, Off. of the Priv. Comm'r of Can., Privacy Commissioner Expresses Support for Proposed Changes to PIPEDA (May 25, 2023), https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230525-2/.

to gain a lead in AI development and establish itself as a global power in the field.[566]

In March 2022, China passed a law aimed at ensuring that information providers do not endanger the country's national security or public interests (including its "Socialist core value[s]").[567] In support of this objective, the law restricts how AI is used by businesses and imposes a stricter oversight regime.[568] It requires companies to provide an explanation when they harm users and to address issues including monopolistic behavior and labor conditions.[569] It also requires recommendation algorithms that have "public opinion characteristics" and "social mobilization capabilities" to complete a filing with the government's algorithm registry system.[570]

In August 2023, a new Chinese law on generative AI came into effect, regulating both training data and model outputs.[571] In November of that year, a Beijing court held that AI-generated content can receive copyright protection[572] in contrast to the U.S. human-authorship approach discussed in Section IV.

In May 2024 the Chinese National Information Security Standardization Technical Committee ("NISSTC") released a draft regulation entitled the Cybersecurity Technology – Basic Security

---

566. Graham Webster et al., Stan. Univ. Digichina, Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017) (Aug. 1, 2017), https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/; Matt Sheehan, Carnegie Endowment for Int'l Peace, China's AI Regulations and How They Get Made (July 10, 2023), https://carnegieendowment.org/2023/07/10/china-s-ai-regulations-and-how-they-get-made-pub-90117.

567. Rogier Creemers et al., Stan. Univ. Digichina, Translation: Internet Information Service Algorithmic Recommendation Management Provisions – Effective March 1, 2022 (Jan. 10, 2022), https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/.

568. Arjun Kharpal, *Chinese tech giants share details of their prized algorithms with top regulator in unprecedented move*, CNBC (Aug. 15, 2022), https://www.cnbc.com/2022/08/15/chinese-tech-giants-share-details-of-their-algorithms-with-regulators.html.

569. Matt Sheehan & Sharon Du, Carnegie Endowment for Int'l Peace, What China's Algorithm Registry Reveals about AI Governance (Dec. 9, 2022), https://carnegieendowment.org/2022/12/09/what-china-s-algorithm-registry-reveals-about-ai-governance-pub-88606.

570. *Id.*

571. Huw Roberts & Emmie Hine, *The future of AI policy in China*, E. Asia F. (Sept. 27, 2023), https://eastasiaforum.org/2023/09/27/the-future-of-ai-policy-in-china/.

572. Keith Kelly, *Computer Love: Beijing Court Finds AI-Generated Image is Copyrightable in Split with United States*, Nat'l L. Rev. (Dec. 4, 2023), https://natlawreview.com/article/computer-love-beijing-court-finds-ai-generated-image-copyrightable-split-united.

Requirements for Generative Artificial Intelligence ("AI") Service (GenAI Security Draft) *which* addresses issues around training data, model integrity, and risk mitigation for generative AI technology.[573]

E. Japan

Japan has followed an alternative, non-regulatory and non-binding approach to AI and issued Social Principles of Human-Centric AI in 2019.[574] The seven AI-related principles outlined in the document focus on human-centricity; education/literacy; protection of privacy; security; fairness in competition; fairness, accountability, and transparency; and innovation.[575] Japan's "Expert Group on How AI Principles Should Be Implemented" underscored that "legally-binding horizontal requirements for AI systems" are "unnecessary at the moment."[576] Accordingly, the country issued sectoral regulations[577] and industry guidance[578] covering the technology but stopped short of enacting regulations to strictly constrain AI.[579]

Japan's Liberal Democratic Party signaled a potential dissent from this strategy in April 2023 when the Promotion of Digital Society Project Team published "The AI White Paper: Japan's National Strategy in the New Era of AI" (the "AI White Paper").[580] It sets forth a national

573. Guilia Interesse, China Releases New Draft Regulations on Generative AI, China Briefing, (May 30, 2024) https://www.china-briefing.com/news/china-releases-new-draft-regulations-on-generative-ai/.

574. LDP Headquarters for the Promotion of Digital Society, Project Team on the Evolution and Implementation of AIs, Japan's National Strategy in the New Era of AI: The AI White Paper (Apr. 2023), https://note.com/api/v2/attachments/download/22d567674279874e2714cbadc79aaf8c; Social Principles of Human-Centric AI (2019), https://www.cas.go.jp/jp/seisaku/jinkouchinou/pdf/humancentricai.pdf.

575. *Id.*

576. Expert Group on How AI Principles Should Be Implemented, AI Governance in Japan Ver. 1.1: Report from the Expert Group on How AI Principles Should Be Implemented (July 9, 2021), https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20210709_8.pdf.

577. Hiroki Habuka, *Japan's Approach to AI Regulation and Its Impact on the 2023 G7 Presidency*, Ctr. for Strategic & Int'l Stud. (Feb. 14, 2023), https://www.csis.org/analysis/japans-approach-ai-regulation-and-its-impact-2023-g7-presidency (noting that, "[f]or example, the Digital Platform Transparency Act imposes requirements on large online malls, app stores, and digital advertising businesses to ensure transparency and fairness in transactions with business users, including the disclosure of key factors determining their search rankings.").

578. *Id.* (noting that "METI's Governance Guidelines for Implementation of AI Principles summarizes the action targets for implementing the Social Principles and how to achieve them with specific examples.").

579. *Id.*

580. The White Paper recognized that LLM technology presents a "New AI Era," that others such as the E.U. and U.S. have been moving forward on regulation, and

strategy that promotes strengthening AI development capacity; active AI utilization in public service; devising policies to encourage and support the use of AI in the private sector; and new approaches to AI regulation. To this last point on approaches, Japan's AI White Paper recommends consideration of regulations for serious risk areas, nimble regulatory modifications to fit the new era of AI, and organization of guidelines for AI utilization in education.[581] Underscoring this proposed change in approach, the paper notes: "the risk of Japan choosing an entirely different regulatory framework from Europe and the US will likely outweigh the benefits in the near future."[582]

In April 2024, Japan put forth voluntary AI Guidelines for Business Version 1.0 which provides definitions, philosophies and principles for instituting responsible AI governance, as well as key considerations for developers, providers and users of AI.[583] In that same month, the United States and Japan announced a series of collaborative initiatives, including a new AI partnership involving major universities and corporations like NVIDIA and Microsoft and several cooperative agreements on AI research and high-performance computing between American and Japanese national laboratories and educational institutions.

F. Singapore

Singapore has taken a proactive approach to fostering a sustainable and trustworthy AI ecosystem.[584] It developed a voluntary governance framework with an outcome-driven, principle-based approach.[585]

To implement its vision, Singapore promulgated three "interlinked initiatives":[586] a "living" and "agile" Model AI Governance

---

that Japan was "lagging" behind in AI adoption. It also noted that "the International Institute for Management Development (IMD) of Switzerland released its global digital competitiveness ranking last September, ranking Japan 29th out of 63 countries surveyed. Japan ranked last in such areas as 'data utilization,' and in many other indicators related to industry, Japan remained in a low position." The AI White Paper: Japan's National Strategy in the New Era of AI, LDP Headquarters for the Promotion of Digital Society, Project Team on the Evolution and Implementation of AIs, Apr. 2023, https://note.com/api/v2/attachments/download/22d567674279874e2714cbadc79aaf8c.

581. LDP HEADQUARTERS FOR THE PROMOTION OF DIGITAL SOCIETY, s*upra* note 574.

582. *Id*. at 19.

583. AI GUIDELINES FOR BUSINESS VER1.0 (Apr. 2024), https://www.soumu.go.jp/main_content/000943087.pdf

584. Yeong Zee Kin, *Singapore's model framework balances innovation and trust in AI*, OECD (June, 24, 2020), https://oecd.ai/en/wonk/singapores-model-framework-to-balance-innovation-and-trust-in-ai.

585. *Id.*

586. *Id.*

Framework,[587] an Advisory Council on the Ethical Use of AI and Data, and a Research Programme on the Governance of AI and Data Use. The Model AI Governance Framework is use case-agnostic and seeks to achieve two overarching principles: promoting explainable, transparent, and fair AI decision-making, and building AI that is human-centric and safe. Alongside the second edition of the Model AI Governance Framework,[588] Singapore published the companion Implementation and Self-Assessment Guide for Organizations[589] and a Compendium of Use Cases[590] to assist companies in their journey toward responsible and trustworthy AI.

In May 2024, Singapore published the Model AI Governance Framework for Generative AI focusing on nine factors-accountability, data, trusted development and deployment, incident reporting, testing and assurance, security, content provenance, safety and alignment Research and development and, AI for the public good- as a voluntary model for how to engender trust in generative AI deployment and use.[591]

G. United Kingdom

The United Kingdom has taken a more industry-favorable, non-binding approach to AI regulation. Their efforts more closely resemble actions taken by Japan and Singapore, in contrast with the EU's horizontal regulation, stratified by AI risk. The UK Department for Science, Innovation and Technology ("DSIT") submitted a white paper on a "pro-innovation approach" to AI regulation in March 2023,[592]

587. Personal Data Prot. Comm'n, Sing., Model Artificial Intelligence Governance Framework (Jan. 2020), https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf.

588. Announcement, Personal Data Prot. Comm'n, Sing., Announcement, Second Edition of Model AI Governance Framework Now Available (Jan. 2020), https://www.pdpc.gov.sg/news-and-events/announcements/2020/01/second-edition-of-model-ai-governance-framework-now-available.

589. Personal Data Prot. Comm'n, Sing., Companion to the Model AI Governance Framework: Implementation and Self-Assessment Guide for Organizations (Jan. 2020), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGIsago.pdf.

590. Personal Data Prot. Comm'n, Sing., Compendium of Use Cases: Practical Illustrations of the Model AI Governance Framework (Jan. 2020), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGAIGovUseCases.pdf.

591. MODEL AI GOVERNANCE FRAMEWORK FOR GENERATIVE AI (May 2024) https://aiverifyfoundation.sg/wp-content/uploads/2024/05/Model-AI-Governance-Framework-for-Generative-AI-May-2024-1-1.pdf.

592. Dep't for Sci., Innovation & Tech., Off. for A.I., U.K., *A pro-innovation approach to AI regulation* (Mar. 29, 2023), https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach.

following a policy paper published in 2022[593] and building on the UK's National AI Strategy.[594]

The DSIT emphasized that the UK will not initially codifyprinciples[595] via statute given the concern that rigid regulations may stifle innovation or reduce the UK's ability to respond to future technological advances.[596] However, the white paper underscores that AI remains subject to existing "context specific" regulations.[597]

The white paper suggests several coordinating actions the UK could undertake to support the framework.[598] The UK Safety Summit in November 2023 was the first of its kind and focused on the risks posed by advanced AI systems, including to biosecurity due to increased information accessibility.[599] The event also explored the positive applications of safe AI, including its potential role in medical advancements and enhancing transport safety. The summit resulted in 28 countries and the EU signing the Bletchley Declaration and signaling their agreement to collectively manage the potential risks of frontier AI and develop the technology in ways that benefit the global community.[600] During the summit, the UK and U.S. also unveiled their respective AI

593. Dep't for Sci., Innovation & Tech., Off. for A.I., U.K., *Policy paper: Establishing a pro-innovation approach to regulating AI* (July 20, 2022), https://www.gov.uk/government/publications/establishing-a-pro-innovation-approach-to-regulating-ai/establishing-a-pro-innovation-approach-to-regulating-ai-policy-statement.

594. Dep't for Sci., Innovation & Tech., Off. for A.I., U.K., National AI Strategy (Dec. 18, 2022), https://www.gov.uk/government/publications/national-ai-strategy/national-ai-strategy-html-version#pillar-3-governing-ai-effectively. A separate study was published in March 2023 on the status of the UK's compute needs, identifying areas of future investment.

595. The pro-innovation framework is underpinned by 5 principles: safety, security and robustness; appropriate transparency and explainability; fairness; accountability and governance; and, contestability and redress. *See* Dep't for Sci., Innovation & Tech., Off. for A.I., U.K., *Policy Paper: A pro-innovation approach to AI regulation* (Aug. 3, 2023), https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper.

596. *Id.*

597. *Id.*

598. These include: coordination of monitoring, assessment of feedback, coherent implementation of principles, support for innovators through regulatory testbeds and sandboxes, provision of guidance to businesses through education and awareness campaigns, monitoring of changes and trends in AI development, and assurance of interoperability with international frameworks. *Id.*

599. News Story, Dep't for Sci., Innovation & Tech., UK government sets out AI Safety Summit ambitions (Sept. 4, 2023), https://www.gov.uk/government/news/uk-government-sets-out-ai-safety-summit-ambitions.

600. News Story, Dep't for Sci., Innovation & Tech., Countries agree to safe and responsible development of frontier AI in landmark Bletchley Declaration (Nov. 1, 2023), https://www.gov.uk/government/news/countries-agree-to-safe-and-responsible-development-of-frontier-ai-in-landmark-bletchley-declaration#:~:text=Leading%20AI%20nations%2C%20convened%20for,by%20frontier%20AI%20and%20the.

Safety institutes to spur international collaboration and lead in the development of AI safety.[601] The two institutes have since signed a Memorandum of Understanding for information sharing, pooling of expertise, and engaging in at least one joint testing exercise.[602]

The global landscape of AI regulation, including policy leadership in the EU, Brazil, Canada, China, Japan, Singapore, and the United Kingdom demonstrates alternate approaches to navigating complex considerations posed by AI technologies. Though diverse, their high-level focus on AI regulation underscores global recognition of the need for comprehensive and adaptive frameworks that balance innovation with ethical considerations, transparency, and accountability. As AI reshapes societies and economies worldwide, the harmonization of international AI frameworks among stakeholders will enable more universal access to its potential while mitigating its risks. As we increasingly operate across borders and our AI use remains agnostic to territorial boundaries we will increasingly require fluency in policy developments across the globe.

Conclusion

Artificial intelligence holds remarkable potential to transform lives and drive innovation, from enabling precision medicine in remote locations to providing personalized tutors for under-resourced students. However, as we explore these novel applications, it is essential to remain vigilant about the associated risks and liabilities. This Article serves as a starting point for identifying and mitigating potential liabilities related to AI.

As AI systems become increasingly embedded in business operations, they are challenging and reshaping the legal landscape. However, it is important to note that they are indeed applicable and governed by our current legal frameworks. AI applications can present complex questions about responsibility for resulting harms. While new regulations are on the horizon—and will indeed be necessary— most questions around AI liability will ultimately be resolved by the courts

601. Press Release, Prime Minister's Off., Prime Minister launches new AI Safety Institute (Nov. 2, 2023), https://www.gov.uk/government/news/prime-minister-launches-new-ai-safety-institute; Press Release, U.S. Dep't of Com., At the Direction of President Biden, Department of Commerce to Establish U.S. Artificial Intelligence Safety Institute to Lead Efforts on AI Safety, (Nov. 1, 2023), https://www.commerce.gov/news/press-releases/2023/11/direction-president-biden-department-commerce-establish-us-artificial.

602. Press Release, Press Release, U.S. Dep't of Com., U.S. and UK Announce Partnership on Science of AI Safety (Apr. 1, 2024), https://www.commerce.gov/news/press-releases/2024/04/us-and-uk-announce-partnership-science-ai-safety.

under existing laws, such as consumer protection, criminal justice and civil rights, privacy, intellectual property, and contracts.

AI does not operate in a regulatory vacuum; rather, it is governed by established legal principles, enforced through case law, and shaped by ongoing policy discussions. Lawyers and executives are well advised to proactively assess current or envisioned uses of AI systems and consider each of the legal frameworks that could be applicable well in advance of their development or deployment of AI to help achieve its promises for a broader cross-section of our population.

All of us have a role to play in ensuring that our AI is trustworthy, safe and invites more opportunity. One of the best guardrails against the misuse of AI is the critical thinking that each of us can apply when we deploy or respond to examples of AI. Lawyers and judges have a particularly critical role in ensuring that AI operates in compliance with our values, as codified in our laws. As highlighted by the ABA, it is a legal duty to ensure that AI technologies comply with emerging laws and to creatively apply existing legal frameworks to these new applications. Similar to past technological advances, lawyers will be on the front lines, developing guardrails and setting limits to ensure AI is equitable for all users.

By staying ahead of potential liabilities and rigorously applying existing legal principles, AI development can be guided to maximize its benefits while minimizing its risks. This vigilance will be crucial in ensuring that AI serves as a tool for progress that aligns with our societal values and legal standards.