

Regulating AI: An Overview Of Federal Efforts

By **Jennifer Maisel** (August 1, 2023, 6:06 PM EDT)

This first part of a two-part series on U.S. regulation of artificial intelligence systems provides an overview and modern context for the existing regulatory, legal and risk management landscape for AI systems in the U.S., built from a network of White House executive orders, federal regulation and federal agency enforcement actions.



Jennifer Maisel

For decades, AI systems have been hiding in plain sight within commercial products across countless industries, with applications in: medical imaging, transportation, communications networks, autonomous vehicles, fraud detection, facial recognition, speech recognition, natural language processing, recommendation engines, spam filters, classification, search, and computer vision.

Likewise, generative AI tools — including those where users directly engage with AI systems to generate content — have been around for a number of years.[1]

As one example, Microsoft Corp. released a conversational AI chatbot, Tay, in 2016, which reportedly took less than 24 hours for Twitter users to corrupt.[2]

The explosion in data, increased processing power of better, faster networked computers and improved algorithms and models has greatly accelerated the advancement of AI systems within the past few years.

For example, in late 2017, researchers introduced the transformer architecture underlying many of the generative large language models used for generative AI chatbots.[3] Diffusion models, such as those used for generative AI image generators, were introduced in 2015.

While AI has been lurking around for a while, it is no longer limited to the purview of computer scientists and businesses with the requisite expertise. Especially with powerful and easy to use generative AI tools now available to the public en masse for endless applications.

With the growth of AI, so too has come increased federal regulatory attention.

Federal Regulation of AI

2019's Executive Order 13859, "Maintaining American Leadership in Artificial Intelligence," jump-started significant, coordinated federal activity focused on balancing the need for regulation of AI with the demands of innovation.

The executive order outlines objectives around AI technology, including promoting research and development, open government data, reducing barriers, technical standards, next generation researchers, and an action plan with several deliverables.[4]

Several key deliverables followed the 2019 executive order, including the Office of Management and Budget's guidance for regulation of AI in the private sector,[5] increased funding and investment in AI,[6] the establishment of National Artificial Intelligence Research Institutes,[7] AI technical standards,[8] and new international AI alliances.

The OMB guidance highlighted 10 binding principles for AI applications: public trust, public

participation, scientific integrity and information quality, risk assessment and management, benefits and costs, flexibility, fairness and nondiscrimination, disclosure and transparency, safety and security, and interagency coordination.

On Feb. 24, 2020, the U.S. Department of Defense adopted ethical principles for AI: responsible, equitable, traceable, reliable and governable.[9]

The National Security Commission on Artificial Intelligence issued a final report in March 2021 explaining importance of AI for national security.[10] Of note, the final report highlights that the "lack of explicit legal protections for data or express policies on data ownership may hinder innovation and collaboration, particularly as technologies evolve."

On Jan. 26, the National Institute of Standards and Technology released the AI Risk Management Framework, along with a companion NIST AI RFM Playbook, AI RMF Explainer Video, AI RMF Roadmap, AI RMF Crosswalk, and various perspectives on the AI RMF from interested organizations and individuals.[11]

The NIST RMF should serve as an instrumental resource for companies looking to develop and commercialize AI systems, and the RMF seeks to promote trustworthy and responsible development and use of AI systems.

Additionally, in October 2022, the White House Office of Science and Technology Policy published "The Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People." [12]

Numerous federal agencies have promulgated guidance and regulations concerning AI systems.

For example, the U.S. Food and Drug Administration, on April 3, published draft guidance for industry and FDA staff — "Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence/Machine Learning (AI/ML)-Enabled Device Software Functions." [13]

The draft concerns regulation of medical device software and other digital health technologies with a focus on safety and efficacy.

The U.S. Patent and Trademark Office and the U.S. Copyright Office have also been examining whether and to what extent existing intellectual property laws adequately address AI systems.

Following the flurry of activity within the executive branch, U.S. Congress enacted four laws in the 116th Congress focused on AI or including AI provisions:

- The National Defense Authorization Act for fiscal year 2021, including the National Artificial Intelligence Initiative Act of 2020;
- The Consolidated Appropriations Act 2021, including the AI in Government Act of 2020, which directed the General Services Administration to create an AI Center of Excellence to facilitate the federal government's adoption of AI technology;
- The Identifying Outputs of Generative Adversarial Networks Act, which supports research on Generative Adversarial Networks, which are used to create deepfakes; and
- The Further Consolidates Appropriations Act, which established a financial program related to exports in AI.

On May 19, 2021, the Congressional Research Service, or CRS, issued a report, "Artificial

Intelligence: Background, Selected Issues, and Policy Considerations," identifying four issues for congressional consideration, including: (1) implications for the U.S. workforce, including job displacement and skill shifts, and the need for an AI expert workforce; (2) federal research and development support and investment in AI; (3) standards development around AI; and (4) ethics, bias, fairness and transparency.[14]

On May 23, the CRS issued a report on "Generative Artificial Intelligence and Data Privacy: A Primer," identifying additional issues for congressional consideration: data privacy and related laws, proposed privacy legislation, existing agency authorities, regulation of data scraping, and research and development for alternative technical approaches.[15]

Among the privacy-related issues, the report highlights that most generative AI applications do not provide notice or acquire consent from individuals to collect and use their data for training purposes, and that Congress may consider requiring generative AI companies to provide an option to opt-out of data collection or mechanisms for users to delete data from existing data sets.

Additionally, the report notes that although no federal laws ban the scraping of publicly available data from the internet, such activity raises privacy concerns — noting the issues around the facial recognition company Clearview AI — and potential competition concerns because larger companies may block competitors from scraping data.

Contrarily, the report simultaneously recognizes that there are some beneficial uses of web scraping by researchers, journalists and civil society groups to conduct research in the public interest.

Congress, however, has not passed comprehensive federal legislation governing the use of AI.

Senate Majority Leader Chuck Schumer is spearheading the congressional effort to craft legislation regulating AI.[16] The potential regulations from Congress would be focused on four guardrails geared toward ensuring responsible AI, requiring: (1) the identification of who trained the algorithm and its intended audience; (2) the disclosure of its data source; (3) an explanation for how it arrives at its responses; and (4) transparent and strong ethical boundaries.

Federal Enforcement Activities

On April 25, the Federal Trade Commission Chair Lina M. Khan and officials from the U.S. Department of Justice, the U.S. Equal Employment Opportunity Commission, and the Consumer Financial Protection Bureau issued a joint statement on AI.[17]

The joint statement confirms that the agencies' existing legal enforcement authorities apply to the use of AI just as they apply to other practices, and that the FTC, DOJ, EEOC and CFPB are among the federal agencies responsible for enforcing civil rights, nondiscrimination, fair competition, consumer protection, and other vitally important legal protections.

The joint statement highlights several examples where the agencies expressed concern about or took action to address potentially harmful uses of AI technology, including: credit decisions, algorithm-based tenant screening services, employment-related decisions about job applicants and employees, invasive forms of commercial surveillance, and tools that have discriminatory impacts.

Critically, the joint letter notes that potential discrimination in automated systems may come from problems with data and data sets, model opacity and access, or "black boxes," and design and use.

The FTC has issued guidance over the past several years regarding the use of AI.[18]

In 2020, the FTC issued guidance urging: transparency, fairness and the ethical use of AI; that enterprises should not deceive consumers regarding AI when using AI tools to interact with customers; that an explanation should be provided where a customer is denied a product or service based on algorithmic decision making; and that firms should validate and revalidate to ensure that models work as intended.[19]

In an April 19, 2021, blog post, the FTC outlined its decades of experience enforcing three laws pertaining to AI systems: (1) Section 5 of the Federal Trade Commission Act, which prohibits unfair

or deceptive practices; (2) the Fair Credit Reporting Act, which may apply when an AI system is used to deny people employment, housing, credit, insurance or other benefits; and (3) the Equal Credit Opportunity Act, which prohibits the use of a biased algorithm that results in credit discrimination. [20]

The FTC has also issued guidance on advertisements about AI systems, cautioning enterprises to be aware of the risks and warning against exaggerating what an AI product can do, promising that an AI product does something better than a non-AI product, or misrepresenting whether a product actually uses AI. [21]

In past investigations and enforcement actions, the FTC has required enterprises to destroy algorithms and other work product trained on data that should not have been collected in the first instance. [22]

The FTC has reportedly opened an investigation into OpenAI, the firm responsible for ChatGPT. [23]

The civil investigative demand focuses on OpenAI's use of information containing personally identifiable information for training its GPT models, and in doing so whether OpenAI has (1) engaged in unfair or deceptive privacy or data security practices or (2) engaged in unfair or deceptive practices relating to risks of harm to consumers in violation of Section 5 of the FTC Act. [24]

Conclusion

The U.S. has been carefully managing a national policy and regulatory ecosystem toward AI systems.

That ecosystem, in balancing the needs for regulation with innovation, has enabled the U.S. to become one of the global leaders in AI technology, rivaled perhaps only by China.

But as AI technology continues to expand into our everyday lives, so too has its risks and the need for regulation. The second part of this series will focus on state legislation and litigation to watch concerning AI systems, and provides practical takeaways.

Jennifer Maisel is a partner at Rothwell Figg Ernst & Manbeck PC.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] For more examples, see my chapter, "AI in Augmented Reality and Entertainment," in the Law of Artificial Intelligence and Smart Machines: Understanding A.I. and the Legal Impact, American Bar Association (released August 2019).

[2] James Vincent, "Twitter Taught Microsoft's AI chatbot to be a racist asshole in less than a day," The Guardian (Mar. 24, 2016), available at <https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist>.

[3] A. Vaswani et al., "Attention is All You Need," 31st Conference on Neural Information Processing Systems (NIPS 2017), available at <https://arxiv.org/pdf/1706.03762.pdf>. For example, the "GPT" model in ChatGPT stands for Generative Pre-trained Transformer.

[4] Exec. Order No. 13,859, available at <https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence>.

[5] Office of Management and Budget Memorandum re. Guidance for Regulation of Artificial Intelligence Applications (Nov. 17, 2020), available at <https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf>.

[6] See the Networking and Information Technology Research and Development (NITRD) Program's

Artificial Intelligence R&D Investments, Fiscal Year 2018-2023, available at <https://www.nitrd.gov/about/>. See also National Artificial Intelligence Research and Development Strategic Plan 2023 Update (May 2023), available at <https://www.whitehouse.gov/wp-content/uploads/2023/05/National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf>.

[7] See National Artificial intelligence (AI) Research Institutes Accelerating Research, Transforming Society, and Growing the American Workforce, available at <https://www.nsf.gov/pubs/2022/nsf22502/nsf22502.pdf>.

[8] See Overview of the National Institute of Standards and Technology's (NIST) AI initiatives, available at <https://www.nist.gov/artificial-intelligence>.

[9] See "DOD Adopts Ethical Principles for Artificial Intelligence," (Release Feb. 24, 2020), available at <https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/>.

[10] See Final Report, National Security Commission on Artificial Intelligence (March 2021), available at <https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf>.

[11] See <https://www.nist.gov/itl/ai-risk-management-framework>.

[12] See <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf>.

[13] See Guidance Document, "Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence/Machine Learning (AI/ML)-Enabled Device Software Functions (April 2023), available at <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/marketing-submission-recommendations-predetermined-change-control-plan-artificial>.

[14] See Congressional Research Service Report, "Artificial Intelligence: Background, Selected Issues, and Policy Considerations," (May 19, 2021), available at <https://crsreports.congress.gov/product/pdf/R/R46795>.

[15] See Congressional Research Service Report, "Generative Artificial Intelligence and Data Privacy: A Primer," (May 23, 2023), available at <https://crsreports.congress.gov/product/pdf/R/R47569>.

[16] See Andrew Solender, Ashley Gold, "Scoop: Schumer lays groundwork for Congress to regulate AI," (Axios, Apr. 13, 2023), available at <https://www.axios.com/2023/04/13/congress-regulate-ai-tech>.

[17] See Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems, available at https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf.

[18] See generally <https://www.ftc.gov/industry/technology/artificial-intelligence>.

[19] See Andrew Smith, "Using Artificial Intelligence and Algorithms," (Business Blog, Apr. 8, 2020), available at <https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms>.

[20] Elisa Jillson, "Aiming for truth, fairness, and equity in your company's use of AI," (FTC Business Blog, April 19, 2021), available at <https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai>.

[21] Michael Atleson, "Keep Your AI Claims in Check" (FTC Business Blog, Feb. 27, 2023), available at <https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check>.

[22] See, e.g., In the Matter of Everalbum, Inc., May 6, 2021, Decision and Order (ordering company to delete all face embeddings derived from biometric information company collected without consent from users' photos and videos), available at

https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_decision_final.pdf.

[23] See, e.g., Cat Zakrzewski, "FTC Investigates OpenAI over Data Leak and ChatGPT's Inaccuracy," *The Washington Post* (July 13, 2023), available at <https://www.washingtonpost.com/technology/2023/07/13/ftc-openai-chatgpt-sam-altman-lina-khan/>.

[24] Federal Trade Commission ("FTC") Civil Investigative Dematnd ("CID") Schedule FTC File No. 232-3044, available at https://www.washingtonpost.com/documents/67a7081c-c770-4f05-a39e-9d02117e50e8.pdf?itid=lk_inline_manual_4.