

Client Alert: Byte-Sized Steps – Navigating the Biden Executive Order on AI and Other Recent Developments in AI Regulation

Publications

October 31, 2023

By: Emily M. Loeb, Caroline Cease, Madeleine Findley, Steve Englund, Benjamin Hand

On October 30, 2023, President Biden signed the Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence (the “Federal AI Executive Order”), a long-awaited executive order that builds upon the Biden Administration’s previously released, non-binding Blueprint for an AI Bill of Rights (“AI Bill of Rights”), and seeks to catalyze both agency action and congressional legislation on artificial intelligence (“AI”) in the coming months. The Federal AI Executive Order is a lengthy document covering myriad concerns that have been raised relating to AI – from cybersecurity to anti-discrimination to competition to competition to intellectual property.

The Federal AI Executive Order, alongside state-level executive activity, such as California Governor Gavin Newsom’s September 2023 Executive Order on AI (the “California AI Executive Order”) reflects the growing consensus that any comprehensive congressional legislation on AI should proceed in a deliberate and careful manner, and, as a result, is unlikely to be enacted in the immediate future. In the interim, with rapid technological advances in AI being measured in months rather than years, concerns continue to grow that AI tools could be used to undermine confidence and reliability in election integrity, world news, and other social and political institutions. The Federal and California AI Executive Orders demonstrate that, even in the face of congressional stasis on AI, the federal and state executive branches will continue to press ahead with action on AI, alongside efforts by state agencies, foreign governments, and international institutions. In addition, also on October 30, the Leaders of the Group of Seven (“G7”) released the Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems (the “Hiroshima AI Code of Conduct”), a set of AI best practices to further promote safe, secure, and trustworthy AI for organizations in the academy, civil society, the private sector, and the public sector working to develop and improve this emerging technology.

There has been, and there will continue to be, much attention on what the Federal AI Executive Order mandates, both inside and outside of the federal government, in the various areas the Federal AI Executive Order touches on. This article offers a different approach, evaluating the Federal AI Executive Order alongside the California AI Executive Order and the G7’s Hiroshima AI Code of

Conduct, to offer a more robust picture of certain key risks and concerns companies should proactively work to mitigate as they build or integrate AI tools into their consumer- or enterprise-facing products and services.

Watermarking and Content Authentication: A lack of effective content authentication and reliable watermarking of AI-generated content remain top of mind for many lawmakers and regulators, especially as the United States heads into the first presidential election cycle in which powerful generative AI tools are widely available to the public. When OpenAI CEO Sam Altman testified before Congress in May 2023, a desire for authentication tools proved to be a key bipartisan concern. That sentiment has not faded. The Federal AI Executive Order requires the Secretary of Commerce to submit a report within 240 days identifying existing tools and best practices for authenticating content, detecting generative content, and watermarking generative content, along with other relevant best practices. That report will be used for, among other purposes, instructing federal agencies on how to label and authenticate content that they create and publish, in order to allow citizens to quickly identify official government communications. This mirrors the non-binding commitment that 15 technology companies made to the Biden Administration in July and September of 2023—promising to, among other protections, develop robust technical mechanisms to ensure that users of their products know when content is AI-generated, including through watermarking systems.

The Hiroshima AI Code of Conduct goes further and proposes that organizations should equip AI systems with content authentication tools that would identify the service or model that created the content, as well as tools that would allow a user to quickly determine if particular content was created through an AI system.

These concerns are ever-present as conflict continues across the globe, with the mere existence and potential for AI-generated content leading people to question the authenticity of images and videos they see. Therefore, companies that provide generative AI tools should actively evaluate how watermarking and other similar disclosure mechanisms can be built into existing or future products and services to mitigate risks. Lawmakers and regulators are likely to remain hyper-focused on the risk of disinformation and manipulation using AI tools, and companies should consider proactively building tools and best practices to mitigate these growing concerns where technically feasible. A proactive approach to identifying and labeling content is likely to serve companies well when high-profile incidents transpire involving AI-generated content, especially where fraught domestic and geopolitical issues are at stake.

Reporting and Investigative Regimes: As more companies build or integrate AI tools into their products and services, companies should simultaneously evaluate how to develop and strengthen their reporting and investigative procedures, both broadly and to prepare for potential future internal and external incidents. Some new reporting regimes will be specific and mandatory. For example, the Federal AI Executive Order invokes the Defense Production Act to require companies developing powerful foundational AI models to notify the federal government about numerous

issues, including when those models are trained, the ownership of the models, the physical and cybersecurity precautions implemented to protect the models, and the results of all relevant red-team safety tests. AI tools used in certain critical infrastructure sectors will also be required to implement red-team safety tests. In light of these and similar requirements, companies should begin to proactively develop and formalize reporting and investigative procedures of internal and external incidents involving AI tools and products. The Hiroshima AI Code of Conduct specifically urges companies and organizations to develop information and reporting mechanisms for incidents before they happen.

Even where reporting and investigative systems are not specifically required, developing appropriate internal systems before problems arise will likely pay long-term dividends for companies in this quickly developing space. The Federal AI Executive Order directs the Department of Justice and federal civil rights enforcers to investigate and prosecute violations related to AI and the Federal Trade Commission, Department of Justice, and other federal regulators have previously made clear that they plan to aggressively enforce existing laws as applied to AI products and tools. For example, in August 2023, the Equal Employment Opportunity Commission settled what is believed to be the Commission's first case involving discrimination in hiring through the use of AI.

State attorneys general and state regulators are also likely to pursue aggressive enforcement actions against emerging AI-related violations of existing laws. Companies that develop reporting and investigative regimes before these incidents arise are likely to be better positioned to successfully navigate federal or state investigations and prosecutions when incidents arise.

Discrimination and Bias: In the same vein, state and federal lawmakers and regulators remain alert to the risk that advances in AI may inadvertently lead to greater discrimination against some groups and communities. The California AI Executive Order specifically tasks state agencies and departments to further analyze the impact use of AI tools may have on vulnerable communities. The Federal AI Executive Order similarly instructs federal agencies to provide clear guidance to federal contractors, landlords, and federal benefits programs regarding requirements to mitigate discrimination in the provision of services, and orders federal regulators to prosecute civil rights violations related to AI.

As more consumer-facing products and services utilize AI systems, companies should pay careful attention to whether best practices are followed to mitigate the risk of discrimination through automated decision-making. Federal regulators and state attorneys general may pursue enforcement actions against companies and industries perceived to be reckless in adopting algorithmic decision-making without proper safeguards against discrimination in place.

Privacy and Civil Liberties: The Federal AI Executive Order reflects concerns that AI may exacerbate risks to privacy, including through its reliance on large quantities of data and its ability to enable linkage of data to identify or make inferences about individuals' identities, locations, habits, and preferences. Federal agencies shall ensure that data collection, use, and retention mitigate

privacy and confidentiality risks, is secure, and incorporates privacy-enhancing technologies when appropriate to combat legal and societal risks from improper collection and use of personal data. The California AI Executive Order likewise tasks state agencies and departments with addressing data privacy and safety considerations related to AI tools, consistent with privacy laws.

Government Procurement: Both the Federal AI Executive Order and California AI Executive Order also demonstrate that where new regulation proves slow or unlikely, standard-setting through government procurement remains a tool for governments to press for desired changes. For example, the California AI Executive Order directs state agencies to issue general guidelines for public sector procurement, uses, and training of generative AI, modeled on the White House's AI Bill of Rights. The Federal AI Executive Order offers more specific guidance, including mandating that federal agencies that fund life-science research require recipients of that funding to follow federal standards for biological synthesis screening to mitigate the risk of AI tools being used to engineer dangerous biological materials. The Federal AI Executive Order also mandates that guidance be issued for the use of AI by federal agencies, including new guidance for AI procurement, and requires federal agencies to develop authentication and watermarking tools for use on content released to the public. By mandating that AI tools used by the government meet these requirements, the White House and California hope that developers of AI tools will also adopt similar practices for their non-government product offerings. Private companies in the procurement space will need to operate with awareness, and be strategic in operation, when it comes to these new rules.

Intellectual Property: The Federal AI Executive Order requires Director of the U.S. Patent and Trademark Office ("USPTO") to publish guidance addressing inventorship and the use of AI, and after completion of an ongoing study of AI-related issues by the U.S. Copyright Office, consult with the Register of Copyrights concerning recommendations to the President on potential executive actions relating to copyright and AI. These recommendations are to address any issues discussed in the Copyright Office's study, including the scope of protection for works produced using AI and the treatment of copyrighted works in AI training. These requirements are much more specific than the Hiroshima AI Code of Conduct, which merely acknowledges that organizations should implement appropriate safeguards to respect intellectual property rights, and the California AI Executive Order, which does not address intellectual property.

Future Legislation: Finally, companies must continue to evaluate future legislative action on AI at both the state and federal levels. Both the Federal AI Executive Order and the California AI Executive Order call for new legislative action on AI. The Federal AI Executive Order in particular calls on Congress to pass appropriate legislation in the AI space, including comprehensive privacy legislation that would help mitigate risks that flow from training AI systems on existing data sets or the use of AI tools by consumers. Although Congress has moved slowly on AI legislation, the combination of new state legislation and concern with disinformation and election integrity may spur federal legislative progress in the coming year. Companies should continue to monitor the

landscape of federal and state legislation on AI and consider what form future legislation might take as they build products and services in this quickly changing space. Our team will be watching and will continue to provide updates.

Related Attorneys



Emily M. Loeb

Partner

eloeb@jenner.com

+1 202 637 6303



Caroline Cease

Partner

ccease@jenner.com

+1 202 639 6056



Madeleine Findley

Partner

mfindley@jenner.com

+1 202 639 6095



Steve Englund

Partner

senglund@jenner.com

+1 202 639 6006



Benjamin Hand

Associate

bhand@jenner.com

+1 415 293 5938

Related Capabilities

Data Privacy and Cybersecurity

Government Controversies and Public Policy Litigation

© 2023 Jenner & Block LLP. Attorney Advertising. Jenner & Block LLP is an Illinois Limited Liability Partnership including professional corporations. This publication, presentation, or event is not intended to provide legal advice but to provide information on legal matters and/or firm news of interest to our clients and colleagues. Readers or attendees should seek specific legal advice before taking any action with respect to matters mentioned in this publication or at this event. The attorney responsible for this communication is Brent E. Kidwell, Jenner & Block LLP, 353 N. Clark Street, Chicago, IL 60654-3456. Prior results do not guarantee a similar outcome. Jenner & Block London LLP, an affiliate of Jenner & Block LLP, is a limited liability partnership established under the laws of the State of Delaware, USA and is authorised and regulated by the Solicitors Regulation Authority with SRA number 615729. Information regarding the data we collect and the rights you have over your data can be found in our Privacy Notice. For further inquiries, please contact dataprotection@jenner.com.

Stay Informed

