Vital Briefing

AI regulation in the U.S.: what it means for corporate and financial services practitioners

By Mark S. Nelson, J.D.

The regulation of artificial intelligence (AI) is likely to consume a significant amount of the federal government's time over the next year now that the Biden Administration has issued a wide-ranging Executive Order calling on federal agencies to use all of their existing authorities to craft guidance and regulations for the oversight of AI generally and for the use of AI by the federal government. The emergence of large language models (LLMs) or generative AI, sometimes referred to as Chat-GPTs, during the preceding year has prompted concern at all levels of the federal government and in Congress regarding the risks and opportunities posed by current and possible future states of AI technology.

That concern also has manifested itself in Europe, where regulators may be the first to adopt AI legislation in the form of the E.U. AI Act by the end of 2023. Although the U.S. started behind other global AI regulators, the Biden Administration's Executive Order may ultimately outpace the early leaders given its much broader scope. Still, the Biden Administration has separately called for Congress to act on related data privacy legislation that has been stalled for several years and Congress could still pursue legislation to enhance federal agencies' existing authorities regarding AI. Meanwhile, attorneys in practices areas touched by AI should not wait for the Biden Administration's EO to be fully implemented before addressing concerns about AI because copious guidance, frameworks, and industry actions already may impact how attorneys respond to AI on behalf of their clients.

Executive Order on AI

The Biden Administration debuted its wide-ranging executive order (EO) on artificial intelligence (AI) on October 30, 2023. The EO addresses AI standards, civil rights, workers, innovation and competition, and the government's own use of AI. The Administration separately called on Congress to pass related bipartisan data privacy legislation. The EO text and a Fact Sheet provide more details about the federal government's expected path toward an ambitious set of AI guidance and regulations.

With respect to fraud, which may impact a number of regulatory practice areas, the EO directs the Commerce Department to issue guidance on authentication and watermarking of AI-generated content. Existing White House guidance would be enhanced in the context of equity and civil rights. In the context of innovation and competition, the FTC will be encouraged to use its authorities to police AI.

Standard-setting for AI will be distributed to multiple agencies, including NIST (red teaming standards), DHS (critical infrastructure and the creation of an AI Safety and Security Board), and to a combination of DoE/DHS (critical infrastructure plus risks posed by AI regarding chemicals, biological materials, radiological materials, nuclear materials, and cybersecurity).

National security, public health, the life sciences, the impact of AI on workers

■ Keeping pace with AI regulation while federal agencies prepare the torrent of guidance mandated by the Biden Administration's EO.

Legislation, guidance, frameworks:
- White House Blueprint for an AI Bill of Rights
- White House Voluntary Commitments on AI risks:
  - Group 1—Amazon, Anthropic, Google, Inflection, Meta, Microsoft, and OpenAI
  - Group 2—Adobe, Cohere, IBM, Nvidia, Palantir, Salesforce, Scale AI, and Stability
- NIST AI Risk Management Framework
- EU AI Act (final version expected late 2023)
- California AB 331

Regulatory activity:
- FTC civil investigative demand sent to OpenAI (as reported by *The Washington Post*)
- SEC predictive analytics proposal

Industry activity:
- Microsoft indemnity agreement
- Google indemnity agreement

(e.g., job displacement and under compensation of workers), and the use of AI by government round out the topics addressed in the EO.

The EO text includes a set of eight principles that the Biden Administration said will guide the government's oversight of AI. The Administration's statements about workers and civil rights were presented with especially strong language. The principles are:

- Artificial Intelligence must be safe and secure.
- Promoting responsible innovation, competition, and collaboration will allow the United States to lead in AI and unlock the technology's potential to solve some of society's most difficult challenges.
- The responsible development and use of AI require a commitment to supporting American workers. Here, the EO stated: "In the workplace itself, AI should not be deployed in ways that undermine rights, worsen job quality, encourage undue worker surveillance, lessen market competition, introduce new health and safety risks, or cause harmful labor-force disruptions."
- Artificial Intelligence policies must be consistent with the Administration's dedication to advancing equity and civil rights. The EO added: "My Administration cannot—and will not—tolerate the use of AI to disadvantage those who are already too often denied equal opportunity and justice."
- The interests of Americans who increasingly use, interact with, or purchase AI and AI-enabled products in their daily lives must be protected.
- Americans' privacy and civil liberties must be protected as AI continues advancing.
- It is important to manage the risks from the Federal Government's own use of AI and increase its internal capacity to regulate, govern, and support responsible use of AI to deliver better results for Americans.
- The Federal Government should lead the way to global societal, economic, and technological progress, as the United States has in previous eras of disruptive innovation and change.

Congress and AI

Past Congressional activity on AI is neither new nor especially far-reaching in terms of what has already been enacted into law. AI-related laws to date have focused on national security and the military, although perhaps one of the more significant results of these initial efforts was to provide a legislative definition of "artificial intelligence." Section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (10 U.S.C. 2358 note), defines "artificial intelligence" as "[a]ny artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets." The definition also includes artificial systems embedded in computer code and physical hardware, cognitive architectures and neural networks, machine learning, and intelligent software agents and embodied robots.

Digital platforms. In the past several years before Congress became concerned about OpenAI's Chat-GPT and similar foundation AI models, Congressional activity focused on reforming the law of digital platforms, largely in response to a felt need to correct past, and to prevent future, errors in the regulation of the Internet and social media. These efforts concentrate on a single comprehensive bill that would also include significant provisions on AI. The Digital Platform Commission Act of 2023 (S. 1671), sponsored by Sens. Michael Bennet (D-Colo) and Peter Welch (D-Vt), would create the Federal Digital Platform Commission to regulate access to, competition, and consumer protection in the digital platform space.

With respect to AI, the DPCA's findings and sense of Congress would state that generative AI has the potential to "magnify" the harms posed by present-day digital platforms, such as jeopardizing local journalism, undermining privacy rights, spreading hate speech, promoting disinformation, and aiding the radicalization of individuals. The bill also would define "algorithmic process" to mean "a computational process, including one derived from machine learning or other artificial intelligence techniques, that processes personal information or other data" for specified purposes, including decision making, content generation, and determining the manner in which information is presented to (or not presented to) users of digital platforms.

AI legislation. Other efforts at regulating AI, some narrow, some grand, emerged over the summer of 2023 when the potential power of Chat-GPT models squarely attracted the attention of lawmakers. The Senate in particular has been actively proposing bills and legislative frameworks to bring oversight to AI.

Two groups of Senators have put forward legislative frameworks for the regulation of AI. The first one, led by Senate Majority Leader Chuck Schumer (D-NY) and a group of bipartisan Senators comprised of Sens. Todd Young (R-Ind), Mike Rounds (R-SD), and Martin Heinrich (D-NM), known as the SAFE Innovation Framework, seeks to ensure America's national security, promote responsible development of AI systems, and preserve democracy in the face of the potential use of AI to manipulate democratic processes. The Schumer framework is short on details and does not appear on its surface to contemplate a singular AI regulatory agency.

By contrast, the Bipartisan Framework for U.S. AI Act, published by Sens. Richard Blumenthal (D-Conn) and Josh Hawley (R-Mo), the Chair and Ranking Members of the Senate Judiciary Committee's Subcommittee on Privacy, Technology, and the Law, does contemplate an

independent oversight body that would administer a registration and licensing regime for the most powerful AI products. The Blumenthal-Hawley framework would provide for the oversight body to bring enforcement actions for violations of the law and would allow for private lawsuits. The Blumenthal-Hawley framework also would address national security, international competition, transparency, and the protection of children and consumers. Moreover, the Blumenthal-Hawley framework would clarify that Section 230 of the Communications Decency Act, the statue that immunizes Internet and social media platforms from most lawsuits over third-party posts, would not apply in the context of AI. The senators also introduced a separate bill (S. 1993) to deny AI platforms such immunity.

Data privacy

Although Section 9 of the EO addresses privacy concerns, the White House separately asked lawmakers to move forward on comprehensive privacy legislation. Much of the interest in data privacy arises from the perception that lawmakers bungled data protection regarding the Internet, especially by adopting Section 230 of the Communications Decency Act, which protects Internet platforms from liability arising from posts made by third parties. Section 230 was part of the larger set of telecommunications reforms enacted in 1996. The subject of data privacy is especially fraught regarding the use of electronic technology by children.

Several other bills introduced in recent sessions of Congress would address different aspects of data privacy on a grander scale. The American Data Privacy and Protection Act (H.R. 8152), introduced in the last Congress by Rep. Frank Pallone

(D-NJ), is perhaps the most comprehensive of the several bills. The bill was reported out of the House Committee on Energy and Commerce in July 2022 by a vote of 53-2. The Congressional Research Service previously summarized and compared the bill to other proposed privacy bills.

> *"I strongly believe that the bedrock of any AI regulation must be privacy legislation that includes data minimization and algorithmic accountability principles," said Rep. Pallone.*

At a recent hearing on AI held by the House Committee on Energy and Commerce, Rep. Pallone emphasized the centrality of data privacy to any future AI regulations. "I strongly believe that the bedrock of any AI regulation must be privacy legislation that includes data minimization and algorithmic accountability principles," said Rep. Pallone. "Simply continuing to provide consumers with only 'notice and consent' rights is wholly insufficient in today's modern digital age."

The Data Privacy Act of 2023 (H.R. 1165), sponsored by Rep. Patrick McHenry (R-NC), would modernize the Gramm-Leach-Bliley Act disclosures that mainly affect banks and securities industry firms. An amended version of the bill was reported out of the House Financial Services Committee in February 2023 by a vote of 26-21.

Lastly, the Upholding Protections for Health and Online Location Data (UPHOLD) Privacy Act of 2023 (S. 631), sponsored by Sen. Amy Klobuchar (D-Minn), would address personally identifiable health and location data. The bill generally would not preempt similar state laws.

With respect to data protection laws already in force, the European Union's GDPR and the California Consumer Privacy Act remain two of the most comprehensive and influential laws for those entities subject to their requirements.

What's next?

During the next year, numerous federal agencies will simultaneously implement the Biden Administration's EO on AI. Practitioners likely can expect multiple opportunities to provide public comments on behalf of clients regarding proposed guidance and regulations. Although the pace and scope of Congressional activity on AI is somewhat challenging to predict with certainty, practitioners should be alert to several legislative streams, including the potential for data privacy legislation that has been called for by the Biden Administration and for a possible first round of AI bills focused on enhancing federal agencies' existing authorities.

Beyond the EO and possible follow-on legislation, practitioners should be alert for agencies, such as the FTC and the SEC, to continue using their existing powers to investigate and regulate aspects of the emerging AI economy. Moreover, practitioners should follow developments in Europe and California because these foreign and state regulators can at times outpace U.S. federal regulators and may present more immediate, and potentially different, compliance risks for some entities.