Legal Perspective

AI in the Supply Chain Under Government Focus

by Jonathan R. Todd, Vanessa I. Gomez, Kristopher J. Chandler, & Megan K. MacCallum


Vanessa I. Gomez


Jonathan R. Todd


Kristopher J. Chandler


Megan K. MacCallum

The U.S. Department of Transportation is seeking input from industry stakeholders on the role of artificial intelligence (AI) in the supply chain. The DOT's Advanced Research Projects Agency—Infrastructure is one of many federal agencies that, together with the White House, are sharply focusing on the risks and opportunities of AI. This example signals the importance of seriously examining the commercial, compliance and national security implications of technological advances.

Five Immediate Areas of DOT Focus on AI

In a recent instance, the DOT requested comments by July 2, 2024, on the safe and responsible development and use of AI in the transportation sector. (See 89 FR 36849.) This inquiry focused on five key areas of concern: (1) Current AI applications in transportation, (2) Opportunities for AI in transportation, (3) Challenges of AI in transportation, (4) Autonomous mobility ecosystems, and (5) Other considerations in the development of AI for transportation. The DOT's request for information also warned against submitting confidential information in response, which understandably highlights the subject's highly sensitive and competitive nature.

Growing Trend of Federal Focus on AI

The federal government has taken a very indirect approach to addressing AI regulation. Like its approach to data privacy and personal information, the federal government has yet to adopt a comprehensive AI law providing compliance obligations for using and deploying AI tools. Instead, they have relied on enforcement by executive agencies of existing laws to address AI. Though there is no current federal omnibus regulation governing the use of AI tools, some federal agencies have clarified that existing statutes and regulations apply to business operations regardless of a business' use of AI tools. This means that if a law applies to your business, using an AI tool will not alleviate your compliance obligations under that law. Again, similar to the approach taken in the US as it relates to data security and privacy of an individual's personal information, to find a comprehensive law on AI, you need to look to individual states for how they are addressing the use and deployment of AI and the legal pitfalls that come with it.

In contrast, the federal government has taken a very hands-on approach to AI usage by federal agencies. In Mar. 2024, the Office of Management and Budget issued its first government-wide policy as memorandum M-24-10 titled "Advanced Governance, Innovation and Risk Management for Agency Use of Artificial Intelligence" (the "AI Memorandum"). Under President Biden's Oct. 2023 AI Executive Order, the AI Memorandum directs federal agencies to "advance AI governance and innovation while managing risks from the use of AI in the federal government, particularly those affecting the rights and safety of the public."

Specifically, the AI Memorandum's requirements and recommendations fall into four categories: (1) Strengthening AI governance, (2) Advancing responsible AI Innovation, (3) Managing risks from the use of AI, and (4) Managing risks in the federal procurement of AI. The risks explicitly addressed are those that "result from any reliance on AI outputs to inform, influence, decide or execute agency decisions or actions, which could undermine the efficacy, safety, equitableness, fairness, transparency, accountability, appropriateness or lawfulness of such decisions or actions. Most of the AI Memorandum applies to "all agencies defined in 44 U.S.C. § 3502(1)," while other provisions only apply to agencies identified in the Chief Financial

Officers Act. Certain requirements do not apply to intelligence community members as defined in 50 U.S.C § 3003. System functionality that "implements or is reliant on" AI that is "developed, used or procured by" the covered agencies is also subject to the AI Memorandum. Activity merely relating to AI, including regulatory actions for nonagency AI use or investigations of AI in an enforcement action and AI deployed as part of a component of a National Security System, are not covered.

The AI Memorandum addresses federal agencies' use of AI and does not extend to the private sector. However, history shows that federal government use and guidance impact the development of best practices adopted by companies. As such, private sector companies using AI will benefit from formally assessing how their current AI practices and policies align with the AI Memorandum and future guidance on the federal government's use of AI.

AI in the Supply Chain Concerns and Implications

Federal interest in exploring AI impacts specific to supply chain services and their national security implications has appropriately taken a broad-based approach. As a comprehensive policy statement, the Biden Administration released its Fact Sheet titled "New Actions to Strengthen America's Supply Chains, Lower Costs for Families and Secure Key Sectors" on Nov. 27, 2023. Among its many recommendations were a Supply Chain Data and Analytics Summit and an AI Hackathon.

The nexus between AI and other emerging technologies and strengthening the domestic United States supply chain in new and novel ways is clear. The 2023 Fact Sheet is one step in a multiyear bipartisan trend of increased recognition that a country's supply chain and national security are one and the same. This trend started before the COVID-19 disruptions, bringing the conversation into national discourse.

Stepping back five years, the Trump Administration's Executive Order 13873 was issued in 2019 to address foreign exploitation of vulnerabilities in the information and communications technology and services supply chain. The concern at that time was that supply chain-related systems and processes were vulnerable to foreign adversaries due to their high-value target status as the veritable backbone of US critical infrastructure. This risk was addressed by assigning responsibility to the Commerce Department for assessing the risk of foreign parties and their domestic actors from acquiring, transferring or dealing in information and technology that could yield catastrophic effects for the homeland. Treasury, State, Defense, Homeland Security and other agencies support Commerce's role in doing so. For example, Homeland Security will be responsible for identifying entities, hardware, software and services that pose vulnerabilities to the US supply chain.

The Biden Administration continued to ramp up the focus on technological applications within the supply chain and their risks. In 2021, the Biden Administration published Executive Order 14034 with the goal of protecting American sensitive data from foreign interference. More recently, on Feb. 28, 2024, the Biden Administration published Executive Order 14117 to expand the scope of national security concerns addressed in 2019 by President Trump. The expanded scope of national security concerns focuses on minimizing access to Americans' bulk sensitive personal data via data brokerages and supply chain agreements pertaining to third-party vendors, employment and investments. The Biden Administration highlights the concern that a supply chain stakeholder in a country of concern must meet compliance obligations to transfer Americans' sensitive personal data to that country of concern's intelligence services. The countries of concern include the People's Republic of China, China's Special Administrative Regions of Hong Kong and Macau, Iran, North Korea, Cuba and Venezuela.

Concerns over international trading relationships and connectivity echo in the recent DOT request for comment and other agency activities. In parallel, Commerce's Bureau of Industry and Security (BIS) has expressed a focus on information and communications technology and services (ICTS) transactions that are essential to the connective vehicles (CV) supply chain. BIS has assessed the potential risks related to the design, manufacturing and implementation of ICTS in CVs due to CV connectivity to original equipment manufacturers, third-party service providers and devices like smartphones. A complex web of geopolitics, federal and state jurisdiction, private industry and consumer interests is emerging.

Private Industry's Path Forward

There is little doubt that interest in AI and adjacent technologies is far from over. The five-year trendline of hardening supply chain protections, particularly from a technological perspective, proves this is not a flash-in-the-pan occurrence. The absence of substantial, comprehensive federal law on the subject does not mean that there are no rules. Instead, this is a moment when nimble multidisciplinary approaches are meaningful. Just as a commercial "arms race" occurs, the best and brightest companies carefully assess emerging best practices, the impact on existing compliance obligations and the threat of geopolitical risks.

»

NOTE: For additional information, please visit: https://www.beneschlaw.com