CLIENT ALERTS & INSIGHTS

Artificial Intelligence Implementation for Supply Chain Applications

JANUARY 13, 2025

Authors: Jonathan R. Todd

Artificial intelligence is under close examination in many industries including the transportation, logistics, warehousing, and supply chain services sectors. The quest for innovation, competitiveness, and organizational efficiency demands at least taking a look. Tangible benefits are by many accounts real for certain uses. Other benefits may be imaginary at least at this point. One challenge for adoption of this technology is the yet-unsettled legal and regulatory framework.

Adoption of AI Technology in Operations

There are many anecdotal stories of deploying artificial intelligence. Some operations have found that AI can perform certain administrative fast quickly, effectively, and with very low error rates.

AI platforms on the market today can review and summarize new service requests, shipping documents, and prepare communications with vendors and customers. AI can help shippers and service providers better manage inventory levels, model anticipated traffic and lanes, and dial-in on fixed and variable costs. All of this is great from perspectives such as speed of execution and cost of overhead.

The operational challenge is that no AI platform is error free. These are not unpaid personnel who do not sleep, eat, or get sick. They are assistants for day-to-day business or strategic planning. Limitations of these technologies can be alarming in the sense that human oversight is required and pro-tech bias must be overcome. These platforms have hallucinations, they don't yet understand human emotion, and they suffer from garbage-in-garbage-out scenarios.

US Legal Considerations for the Industry

Legal challenges for adoption of AI range from typical software license concerns to national security and data privacy. In some ways these platforms are no different than any other licensed system. You expect that it will work consistent with your service level agreement. You expect that it will not infringe or misappropriate any other party's intellectual property or misuse your proprietary information, which can be risks for this technology. You also expect that you will own and be free to use the outputs of this technology, which can also be a risk.

Some concerns extend far beyond your organization. The White House issued an Executive Order in 2023 focused on agency use of AI in ways that will protect the rights and safety of the public. The White House also issued a memorandum in 2024 intended to drive adoption of the technology, doing so responsibly, managing risks inherent in the technology, and managing risk in federal procurement of the platforms. If there is a future where private sector regulation is rolled out these early indicators this may well serve as a framework.

Supply chain focused agencies are also taking notice. The Department of Transportation is investigating development and use of AI in the space. In the fact-finding stage this effort focused on current AI applications, opportunities for future applications, challenges of implementation specific to the transportation sector, and implications for autonomous mobility. Broader supply chain applications are also receiving attention. The White House released a Fact Sheet in 2023 that identified supply chain risks and opportunities including by recommending an AI Hackathon for supply chain applications. At the same time a dizzying array of export restrictions and sanctions have unfolded over the course of the Biden Administration to thwart perceived geopolitical threats as countries like China, Russia, Iran, and North Korea develop and seek access to critical technologies.

Foreign Legal Considerations for All Industries

Among our foreign allies the European Union is taking a more fulsome approach to AI regulation. The EU AI Act went into force in 2024 with an effective compliance date of 2026. The AI Act will apply to companies producing AI technology and to its users. Exploitative biometric and social scoring systems are prohibited. High risk systems including those deployed in some transportation applications will be required to conduct periodic risk assessments while increasing safeguards around cybersecurity and data privacy. Fines for compliance failures may reach up to 35 Million Euros or 7% of global revenue.

Navigating Through the Unknowns

Planning is the key to navigating these uncharted waters for domestic US businesses. It is more important than ever for technology leadership to identify appropriate roles within organizations, manage the procurement and contracting for these systems, thoughtfully implement to maximize ROI, and actively guard against the risks of poor output as well as threat actors and legal compliance. Fortunately, many in the industry should be on a good foundation to begin or continue these activities. For example, some segments of the industry are required by the TSA to appoint cybersecurity coordinators due to the increased activity by threat actors. Those segments typically include operations by air carriers, indirect air carriers, certain rail lines, and certain passenger carriers. AI represents one more complexity for industry technology professionals that will only grow in impact for years to come.

Jonathan Todd is Vice Chair of the Transportation & Logistics Practice Group at Benesch Law. He may be reached at 216-363-4658 or jtodd@beneschlaw.com.