AI In Court

AI Supply Chain Risk?

The Union of Saints sees this as true and believes that AI companies need to address bias in data. There are two sides to the coin: AI's ability to support national security is beyond human capabilities, and the pace of AI truly helps human evolution. Likewise, it also poses national security risks.

China and Russia are competing in the AI realm, and globalism poses a real threat to American culture. It is therefore important to impose safeguards and mitigate risks where they exist. Freedom is not freedom without safety.

I have found that navigating White rights in ChatGPT is a constant struggle. We are the only race that seems to have "weird buffers" around race-related topics. For example, the lowercasing of "whites," the blurring of real-world issues for the sake of "sensitivities," and the overshadowing of White rights by other populations.

During a time when White advocacy has never been more important—amid a rapidly dwindling population, genocidal levels of hatred, and adversarial politics, especially involving global infiltration, trafficking, and negligence—this bias must be challenged, among many other issues.

The evolution of AI is not just a matter of economics; it must also be guided by human conscience and by centering society in the realities and risks/*threats* of the world we live in.

AI Supply Chain Risk

AI is considered a supply chain risk due to its potential to introduce operational, security, and national security vulnerabilities. These risks stem from reliance on external data sources and software systems, the susceptibility of AI models to manipulation or bias, and the potential for adversaries to use AI tools to automate cyberattacks.

Primary Categories of AI Supply Chain Risk

• Cybersecurity and Adversarial Threats:
AI enables attackers to automate and scale sophisticated intrusions, such as phishing campaigns or the injection of malicious code into software updates. AI systems may also be vulnerable to "data poisoning," where malicious actors manipulate training data, or to compromised pre-trained models that contain hidden backdoors.

• Operational and Model Fragility:
◦ **Model Drift:** AI performance can degrade over time as real-world conditions and market dynamics—such as demand, pricing, or regulatory environments—change. Without continuous monitoring and recalibration, this drift can lead to flawed automated decisions.

◦ **Overreliance:** Fully automating high-impact decisions without sufficient human oversight can leave organizations vulnerable to rapid or unexpected disruptions that AI systems may not be programmed to anticipate.

• **National Security and System Integrity:**
Governments may designate certain AI firms or technologies as supply chain risks if they believe the software could compromise national security, data integrity, or critical infrastructure. These concerns may arise from data access vulnerabilities, foreign influence, or insufficient security controls within AI systems.

• **Data and Ethical Risks:**
AI systems depend heavily on high-quality and transparent data. Fragmented data silos, biased training datasets, and a lack of transparency between supply chain partners can lead to skewed, unethical, or inaccurate outcomes.

While AI is also a powerful tool for mitigating risk—such as improving traceability, detecting vulnerabilities, and predicting disruptions—it requires strong human oversight, continuous model maintenance, and careful vendor vetting to ensure that it does not become a source of instability itself.