TOP 5 TAKEAWAYS FROM SESSION III:

Mitigating Liability Risks When AI Goes Wrong

Association of Corporate Counsel Northeast Chapter,
"Unlocking the Algorithm: AI from the In-house Counsel's Desk" — June 6, 2025

1. Incorporate Cybersecurity Standards

As companies race to deploy AI tools, often due to pressure from the C-suite, investors, and shareholders, they need to ensure that they do not cut corners that create cybersecurity risks and increase the likelihood of a data breach. At a minimum, AI systems should incorporate the same level of cybersecurity standards (e.g., access controls, encryption data requirements, intrusion detection and monitoring, etc.) as any other tool in an organization's network because they expand the potential entry points for malicious actors and increase vulnerability risks. It is therefore imperative that organizations continuously monitor their AI applications and infrastructure to detect any irregularities and potential security breaches such as data poisoning, data manipulation, leakage of personal or confidential information, and misuse.

2. Adopt AI Governance Controls

Block users on your network from using risky generative AI (GenAI) tools such as the DeepSeek AI model, which contains serious security flaws, vulnerabilities, and stores user data on servers in China. When China's DeepSeek shocked the world with its announcement in late January 2025 that it had developed a comparable model to ChatGPT, millions of people around the world rushed to download this app and experiment with it. Such activity could cause serious harm to your organization from the leakage of confidential and proprietary data. Organizations should clearly set out rules and boundaries in their AI Acceptable Use policy on what specific types of AI tools are permitted and that any use of AI tools needs to comply with all applicable laws and regulations. Organizations should further monitor user behavior with regards to how AI tools are being used and what information is being input into any publicly available AI tool.

3. Reduce the Likelihood of Government Enforcement Actions and False Claims Act (FCA) Liability

Government agencies have begun closely scrutinizing the use of AI tools and cracking down on misleading, deceptive, or unfair trade practices in connection with AI technology. Numerous enforcement actions have been brought by the U.S. Federal Trade Commission and Securities Exchange Commission against companies for issuing false and misleading statements about the capabilities of their AI systems, a practice that is referred to as "AI-Washing." The Department of Justice is likely to target AI-powered healthcare billing and coding systems in its push to prosecute health care fraud, which it recently announced was the top white-collar fraud priority under Attorney General Bondi.

Errors in automated coding and claim submissions to the government can result in liability under the FCA leading to treble damages. Similarly, predictive diagnostic AI tools may influence medical practitioners resulting in upcoding and overbilling practices. To reduce liability risk, organizations should ensure that they can demonstrate that they acted reasonably in implementing and overseeing AI systems, conducted robust risk assessments, regularly audit and monitor AI tools, and promptly investigate, correct, and remediate any identified discrepancies or errors.

4. Take Steps to Address the Rise in Lawsuits Involving AI Tools

AI tools can go wrong, make mistakes, and cause harm. Since the launch of GenAI, there has been a steady increase in the number of lawsuits being filed involving the misuse of AI tools. For instance, failure to implement guardrails in an AI system and monitor AI outputs can prove catastrophic and provide the basis for a product liability claim. On May 21, 2025, U.S. District Judge Anne C. Conway for the Middle District of Florida denied a motion to dismiss and allowed a lawsuit accusing Google and Character.AI of causing a 14-year old's suicide after he became addicted to an AI chatbot to move forward, finding "the alleged design defects" actionable. On June 4, 2025, Reddit sued AI startup Anthropic in California State Court for unlawfully using its data for commercial purposes without paying for it and in violation of Reddit's user data policy. It is only a matter of time before we see legal malpractice claims against lawyers for filing pleadings with hallucinated legal citations. Once a problem with an AI tool is detected, steps should promptly be taken to investigate the issue, preserve the evidence, consider making a voluntary self-disclosure and make any required disclosures to state and federal agencies, and fully remediate the situation.

5. And Get Ready for the Challenges of Agentic AI

AI agents powered by large language models are not only generating new content in response to prompts, but autonomously making and executing decisions. Agentic AI has the potential to transform business operations. AI agents, however, could also increase liability risks while also making organizations more susceptible to cyberattacks. AI agents are authenticated users on a network that operate using corporate credentials and rapidly execute decisions. They can be tricked and manipulated by a prompt injection or adversarial action. It is therefore crucial to adopt clear policies, safeguards, oversight frameworks, and auditing procedures, and conduct AI red teaming exercises.

Contact Us:

For additional information related to this article, please contact **B. Stephanie Siegmann**, your Hinckley Allen attorney, or any of our attorneys.

B. Stephanie Siegmann, Partner
617-378-4181
ssiegmann@hinckleyallen.com

© 2025 Hinckley, Allen & Snyder LLP. All rights reserved. Attorney Advertising.