Insights: Publications

5 Key Takeaways | The Law of the Machine (Learning): Solving Complex AI Challenges

September 15, 2025

As businesses are under increasing pressure to develop and deploy artificial intelligence (AI) tools, their legal departments are facing new challenges at this intersection of innovation, compliance, and risk. Recently, Kilpatrick's **Mike Breslin**, **Meghan Farmer**, and **Greg Silberman** joined Rome Perlman, Associate General Counsel, National Student Clearinghouse, to explore some of the more subtle and complex issues in the AI legal landscape and provide practical tips for in-house counsel who need to quickly assess and manage their clients' use and deployment of advanced AI systems. The discussion, sponsored by the Association of Corporate Counsel (ACC) Capital Region Chapter, addressed these topics through the lenses of risk management, regulatory compliance, data privacy, model governance, contracting considerations, and incident classification and response.

Mike, Meghan, and Greg offer the following takeaways from the discussion:

1. Data Underpins Model Performance, Governance, and Risk Mitigation.

High-quality, well-managed data ensures AI model reliability, drives continuous improvement, and provides meaningful context. Establish data management protocols that address collection, storage, processing, and disposal, embed privacy-by-design and track data provenance. Use robust data controls to enable governance, support compliance, and build trust in AI systems.

2. Responsible AI Requires Accountability, Transparency, and Human Oversight.

Organizations must assess AI systems for impact, identify adverse effects, and design for informed human control. Provide clear disclosures about AI capabilities and limitations, and state when content or interactions are AI-generated. Human oversight and regular policy reviews are vital to maintaining ethical and compliant AI use.

3. Classify and Respond to AI Incidents to Manage Risk Effectively.

AI incidents are not just another type of cybersecurity incident. Systematically classifying by domain, root cause, lifecycle stage, and responsible owner is critical for effective response. This enables prompt containment, accurate evidence preservation, clear accountability, and tailored remediation. Apply consistent classification to support trend analysis and continuous improvement across teams.

4. Adopt Best Practices in AI Contracting.

Define permitted uses, clearly allocate IP ownership and data training rights, mandate data governance and privacy compliance, and set performance and bias standards. Require transparency, audit rights, and termination provisions for compliance failures. Continuously monitor contract performance and regulatory developments to manage evolving risks.

5. Implement Practical Controls and Education for Safe, Fair, and Effective AI Use.

Mitigate AI risks with layered controls, including human oversight, privacy-by-design, secure coding, data provenance tracking, and documented policies. Train employees regularly on AI policies, known limitations (such as hallucinations and data retention), and verification of AI outputs. Regularly review and update policies to address new risks.

For more information, please contact:
Mike Breslin, mbreslin@ktslaw.com
Meghan Farmer, mfarmer@ktslaw.com
Greg Silberman, gsilberman@ktslaw.com

Related People

Michael J. Breslin

t 404.685.6752
mbreslin@ktslaw.com

Meghan K. Farmer

t 404.541.6816
mfarmer@ktslaw.com

Gregory P. Silberman

t 650.462.5310
gsilberman@ktslaw.com