

MAYER | BROWN

AI SUMMIT 2025

Los Angeles



VIEW ONLINE MATERIALS

AGENDA

SEPTEMBER 18, 2025

1:15 – 2:00 P.M.	PANEL 1: AI GOVERNANCE <ul style="list-style-type: none">• How to structure an organization's AI oversight team<ul style="list-style-type: none">◦ Cross-disciplinary group◦ HR, IP, Privacy, Cyber, Engineer, Data Scientist, etc.◦ Training in regular cadence• Approaches organizations take to address AI regulations and frameworks as part of their AI governance program<ul style="list-style-type: none">◦ Establishing an AI governance framework◦ Mapping AI Use cases to regulatory risk◦ Implementing policies• Issues organizations deal with when developing & deploying an AI system<ul style="list-style-type: none">◦ Data privacy◦ Bias, Discrimination & fairness◦ IP issues◦ Liability and contractual risks◦ Cross-border variance in data transfer laws
2:00 – 2:15 P.M.	NETWORKING BREAK
2:15 – 3:00 P.M.	PANEL 2: AI AND ANTITRUST <ul style="list-style-type: none">• Introduction• Courts and regulators keeping up with pace of AI<ul style="list-style-type: none">◦ Enforcement actions◦ Civil litigation◦ Regulation as a proactive approach and DOJ compliance guidance• Disruption and Antitrust<ul style="list-style-type: none">◦ The Digital Markets Act◦ Algorithmic pricing◦ Practical considerations for businesses• International Antitrust & AI<ul style="list-style-type: none">◦ G7 Competition Authorities• Industrial Policy and AI<ul style="list-style-type: none">◦ AI-related competition enforcement decisions on national security• Closing remarks - what are the AI issues in your space that keep you up at night?
3:00 – 3:45 P.M.	PANEL 3: INTELLECTUAL PROPERTY <p>Copyright Claims and Fair Use Defense</p> <ul style="list-style-type: none">• Recent court rulings to copyright claims involving artificial intelligence<ul style="list-style-type: none">◦ ROSS AI decision◦ Recent rulings involving Anthropic and Meta

	<ul style="list-style-type: none"> • Fair use factors most likely to support a fair use defense for the training of AI models • Potential viability of a fair use defense for generative AI models vs. non-generative AI • Best practices of developers of AI systems to best position themselves for a viable fair use defense • U.S. Copyright Office and recent court opinions <p>Ownership of AI-Generated Materials</p> <ul style="list-style-type: none"> • AI produced work <ul style="list-style-type: none"> ◦ Who should be deemed the “author” for purposes of U.S. copyright law, and why? ◦ Who should be the “inventor” under patent law? • Human input necessary for a work to be protected under IP law and lines to be determined • Determining ownership shares in the case of works generated with a combination of AI and significant human input • Contractual provisions for consideration <p>Current Legal Landscape</p> <ul style="list-style-type: none"> • Recommendations for continued guidance on the developments in this area • Who is best equipped to address the rapidly evolving landscape? Courts? Legislatures? Industry customs and practices? • Advantages and disadvantages of licensing training data • How can intellectual property law balance the potential benefits and innovations made possible through AI with the protection of rightsholders’ ownership interests? <p>Emerging Legislative and Regulatory Framework</p> <ul style="list-style-type: none"> • Copyright Office’s guidance on additional legislation • Should federal legislation mandate transparency regarding the data used to train AI models and, if so, what enforcement mechanisms would be both practical and respectful of privacy? • Varying approaches to AI regulation in different countries and regions for multinationals • Prospects for an international treaty addressing AI and IP
3:45 – 4:00 P.M.	NETWORKING BREAK 2
4:00 – 4:45 P.M.	<p>PANEL 4: CONTRACTING FOR AI</p> <p>Introduction & Context</p> <p>Perspectives on AI Contracting Challenges</p> <ul style="list-style-type: none"> • Intellectual Property • Compliance • IP Infringement • Performance Warranties and SLAs <p>Liability and Risk Allocation</p> <ul style="list-style-type: none"> • Excluding indirect/consequential damages and cap direct damages • Liability

	<ul style="list-style-type: none"> • Indemnification <p>Agentic AI</p> <p>Quick Hits</p> <ul style="list-style-type: none"> • Data Privacy and Security • Transparency & Explainability • Bias and Ethical Use • Termination Clauses <p>Looking Forward: Trends & Final Thoughts</p>
4:45 – 5:30 P.M.	<p>PANEL 5: SECURITY CHALLENGES</p> <ul style="list-style-type: none"> • Intro and overview of the multifaceted security challenges posed by AI • Key cybersecurity issues associated with AI <ul style="list-style-type: none"> ○ AI-Powered Cyber attacks ○ Deepfakes ○ AI-powered phishing campaigns ○ AI-enhanced cyber attacks • Key national security issues associated with AI <ul style="list-style-type: none"> ○ Government support for the use of AI for security ○ Data security ○ Application security ○ Model/model weight security ○ Infrastructure security ○ Securing AI output (code development) • Approaches companies can use to mitigate these risks <ul style="list-style-type: none"> ○ Expectations for developers ○ Expectations for deployers ○ Testing AI security ○ Responding to incidents
5:30 – 7:30 P.M.	RECEPTION