Webinar

Corporate AI: Navigating Legal and Compliance Risks

February 10, 2026

Ad Idem Network

X1

Kelly Twigger

Minerva26
CEO & Founder

ESI Attorneys
Principal

Kelly Twigger is a seasoned attorney, expert consultant, and thought leader in eDiscovery, legal technology, and data management for litigation. As Principal at ESI Attorneys, she leads a boutique firm advising law firms, corporations, and municipalities on eDiscovery, privacy, cybersecurity, and information governance.

Kelly is also the CEO of Minerva26, a SaaS strategic command center for litigators. Recognized as a Fastcase 50 Honoree and an ABA Woman in LegalTech, she also teaches eDiscovery at the University of Colorado Law School.

Christina Wojcik

Pierson Ferdinand LLP

Chief Innovation Officer

Christina Wojcik is a dynamic leader at the intersection of law, technology, and innovation. As Chief Innovation Office at Pierson Ferdinand LLP, she drives the firm's adoption of cutting-edge legal technologies, including AI-powered tools, to deliver more efficient and client-centered solutions. Christina is the former head of Innovation and Technology for Citibank's Global Legal Department, a Practice Executive at IBM and has supported three companies from early stage through exit by acquisition.

Christina's professional brand is rooted in visionary strategy, radical inclusivity, and forward-thinking leadership. A recognized thought leader, Christina frequently speaks and writes about the future of legal services, with a focus on how generative AI and data-driven insights can transform legal, compliance, and risk management.

Landon Speights

Pierson Ferdinand LLP

Founding Partner and CISO

Landon Speights is the Founding Partner of Pierson Ferdinand and brings nearly two decades of experience advising clients across complex litigation, regulatory, and high-stakes legal matters. He has served in multiple leadership roles, including Managing Partner, Co-Global General Counsel, and currently Deputy General Counsel, helping shape the firm’s strategic and operational foundation. In addition to his legal practice, Landon serves as the firm’s Chief Information Security Officer, leading cybersecurity strategy, risk management, and data protection initiatives. His work sits at the intersection of law, technology, and professional responsibility is grounded in real-world governance, ethics, and risk mitigation—not theory.

John Patzakis

X1

Executive Chairman and CLO

John Patzakis is the Executive Chairman of the Board and Chief Legal Officer at X1. He has an extensive background and expertise in enterprise software, eDiscovery and corporate compliance, combining strong knowledge of both the law and the supporting technologies in those areas.

Prior to joining X1, John served nearly a decade at Guidance Software, Inc, as a co-founder and senior executive. Prior to joining Guidance, John spent eight years practicing law in the fields of commercial litigation and business transactions.

Today's Discussion

- Overview of AI Legal and Compliance Risks
- eDiscovery and Litigation Exposure
- Ethical Obligations for Lawyers Using AI
- Trade Secret and Confidentiality Considerations
- AI Security Best Practices for Effective Corporate Governance
- Key Takeaways and Risk Management Recommendations
- Questions

Corporate AI: Trade Secret Risk

- Federal law requires “reasonable measures” to maintain secrecy of trade secret information.
- Feeding proprietary source code or technical data into AI without security and privacy measures may jeopardize trade secret protection.
- *Snyder v. Beam Technologies, Inc.* (10th Cir. 2025) – Failure to secure confidential data and use confidentiality protections defeated trade secret claims.

eDiscovery Exposure and AI Interactions

- AI prompts and responses may constitute discoverable electronically stored information (ESI).
- *In re OpenAI, Inc. Copyright Infringement Litig*. (S.D.N.Y. Dec. 2, 2025)
  - Litigation highlighted potential discoverability of AI prompts and system interactions.
  - Courts increasingly view AI generated content as business records or evidence.
  - Organizations must consider retention, preservation, and review obligations.
- Proposed Federal Rule of Evidence 707 – Machine-Generated Evidence
  - Machine-generated evidence may require satisfaction of Rule 702 reliability standards.
  - Public comment period open through February 16, 2026.

eDiscovery Exposure: Microsoft Co-Pilot

- Microsoft confirms Copilot interactions are logged through Microsoft Purview unified audit logs.
- Prompts and responses can be searched, preserved, and produced through Purview eDiscovery tools.
- AI chats may be treated similarly to emails or internal documents in litigation or regulatory investigations.
- Prompts and outputs may become subject to legal holds and production obligations.
- Potential exposure of privileged, confidential, or sensitive business information.

Key AI-Related Ethics Opinions

American Bar Association SCEPR Formal Ethics Opinion 512 (July 29, 2024)

To ensure clients are protected, lawyers using generative artificial intelligence tools must fully consider their applicable ethical obligations, including their duties to provide competent legal representation, to protect client information…:

NYC Bar Assn. Formal Opinion 2025-6

"[A]ttorneys should advise clients of the risks of the loss of confidentiality and privilege, particularly, …, where clients are using their own AI tools. … Because the storage of information obtained by client AI tools will not be under the attorneys' control, they should advise clients of the risks of the loss of confidentiality and privilege."

Ten Commandments of AI Ethics for Attorneys

1. Lawyers Must Retain Professional Judgment
2. Lawyers Must Stay Technologically Competent
3. All AI Output Must Be Verified
4. Client Confidentiality Must Be Protected
5. Disclosure Is Required When Rules or Courts Demand It
6. Lawyers Must Supervise AI Use
7. Bias and Harm Must Be Addressed
8. Courts, Clients, and Opposing Parties Must Not Be Misled
9. Billing Must Be Fair and Transparent
10. Follow Local Laws, Ethics Rules, and Court Orders Control

Law Firm Requirements for Secure AI Deployment

- Leverage AI to enhance efficiency, research, document review, and client service.
- Implement strong confidentiality safeguards and secure client data handling.
- Adopt vetted, enterprise-grade AI solutions with security and audit capabilities.
- Develop internal policies governing acceptable AI usage.
- Provide attorney training on AI risks, ethical duties, and confidentiality obligations.
- Conduct vendor risk assessments for third-party AI platforms.

Questions to Ask for a Secure AI Deployment

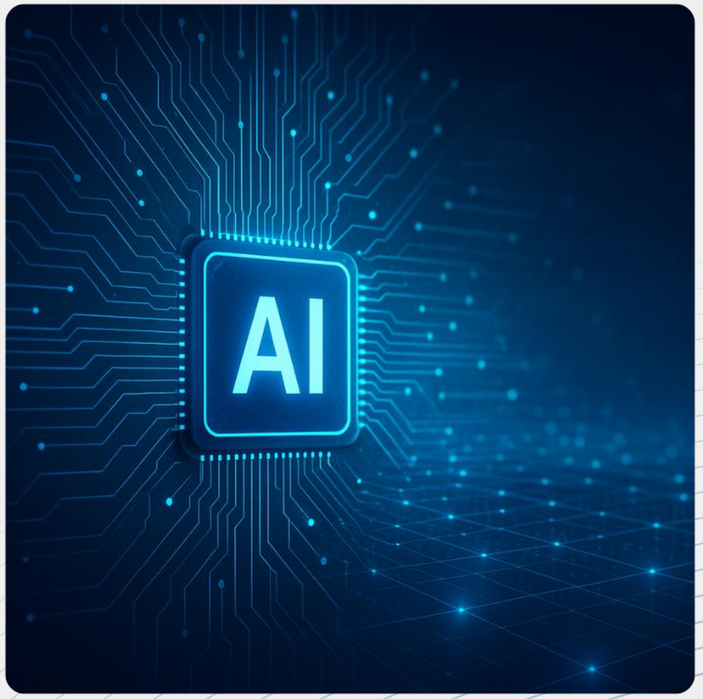
1. What specific problem are we solving, and does AI materially improve the outcome?
2. What data will the AI system access, process, or store?
3. How does the vendor handle data ownership, retention, and reuse?
4. What security controls protect the AI system and its data?
5. How accurate is the system, and how are errors identified and corrected?

Questions to Ask for a Secure AI Deployment

6. What are the known limitations, failure modes, and bias risks?
7. Who remains accountable for decisions influenced by the AI?
8. Does the AI use comply with ethical rules, court orders, and professional obligations?
9. How will this AI be governed, monitored, and audited over time?
10. What is our exit strategy if the AI tool fails or creates risk?

Corporate AI Safeguards

- Develop policies and procedures to protect security and confidentiality when using AI.
- Educate employees and in-house counsel regarding AI risk mitigation responsibilities.
- Implement governance controls including approval workflows and monitoring mechanisms.
- Not all AI poses equal risk.
  - Higher risk AI involves sensitive, proprietary, or regulated data requiring enhanced safeguards.
  - Lower risk AI may involve public or non-sensitive operational use cases.



Corporate AI Deployment Strategies

- Understanding Basic AI Architecture
  - LLMs are the Brains of AI.
- Consider Utilizing/Hiring Internal AI Expertise to Develop and Curate Models.
- Deployment Architectures Are Extremely Important
  - Consider in-place AI deployment within corporate networks or controlled environments.
  - In-place AI can reduce trade secret leakage, limit third-party discovery exposure, and enhance privacy and audit control.
  - Secure deployment enables organizations to realize AI benefits while maintaining compliance.

13th Annual UF Law E-Discovery Conference

Event available to legal professionals worldwide. Register for the **virtual experience** of the UF Law E-Discovery Conference, free for anyone working, studying, or practicing in the legal field.

Details:

- February 25 & February 26, 2026
- Free virtually
- CLE and continuing education credits
- For more information visit: *www.ufediscoveryconference.com*

Questions

Thank You for Attending!

Canby Wood | Ad Idem Network

Kelly Twigger
Minerva26
minerva26.com
kelly.twigger@minerva26.com

Christina Wojcik
Pierson Ferdinand
pierferd.com
christina.wojcik@pierferd.com

Landon Speights
Pierson Ferdinand
pierferd.com
landon.speights@pierferd.com

John Patzakis
X1
X1.com
jpatzakis@x1.com