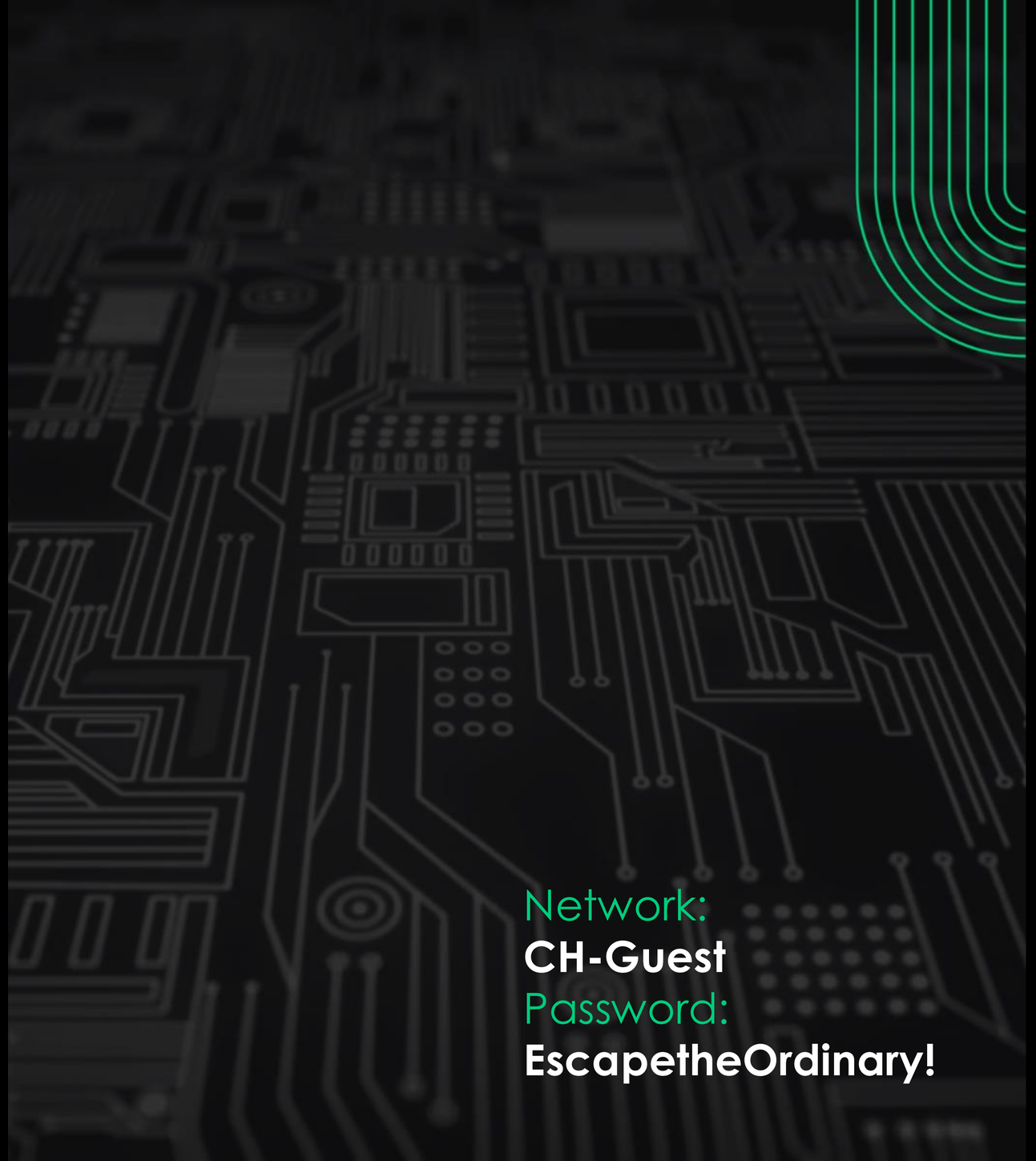
2026 Data Privacy & Cybersecurity Law Summit - Chicago

April 28, 2026

Presented by Clark Hill



Network:
CH-Guest
Password:
EscapetheOrdinary!

Agenda

- **8:00 a.m.** – Registration and Breakfast
- **8:30 a.m.** – **Cybersecurity & Privacy in 2026: What Keeps Executives Up at Night**
- **9:30 a.m.** – Break
- **9:40 a.m.** – **Artificial Intelligence Meets the Courtroom: Emerging Risks in Modern Litigation**
- **10:40 a.m.** – Break
- **10:50 a.m.** – **Roundtable Discussion**
- **12:00 p.m.** – Open Networking
- **12:30 p.m.** – Program Concludes

Reminders

- Pending approval for 2 hours of CLE with Illinois State Bar
- To receive CLE credit, please complete and sign the form before exiting.
- 10-minute break between each session
- Breakfast, coffee and drinks available in the lobby
- Restrooms to the right as you exit the conference room
- Digital copies of slides will be emailed following today’s program

Cybersecurity & Privacy in 2026: What Keeps Executives Up at Night

Presenters:

Melissa Ventrone, Member, Clark Hill
Mike Co-Founder and Partner, Enduir

April 28, 2026


What Keeps You Up At Night?

Agenda: What Keeps You Up At Night?

- AI, AI, and More AI
- Cyberattacks, Including Ransomware and Data Exfiltration
- Supply Chain Risk – What Are Our Vendors Doing?
- Legal and Regulatory Pressures – just how many laws are there?
- Executive and Board Accountability
- Practical Tips to Address the Sleepless Nights

AI, AI and More AI

Different categories of risk as it pertains to AI:

- Technical risk –e.g., cyberattacks
- Organizational misuse of AI
- Operational reliance on AI
- Legal risks
- Unknows – what else?

Technical Risk From AI

- Generative AI used for :
  - Sophisticated phishing
  - Automated vulnerability discovery
  - Highly effective reconnaissance
- Mythos and GPT 5.4

AI as Threat. AI as Target.

AI expands the attack surface in two directions. Adversaries weaponize external AI to attack the enterprise, and adversaries exploit the AI we deploy to attack from within. Each carries distinct legal and disclosure exposure.

Adversaries Using AI Against Us

- Deepfake voice and video impersonation enabling executive fraud and unauthorized fund transfer
- Automated vulnerability discovery and exploit generation, compressing patch and notification windows
- Hyper personalized phishing produced at machine speed and scale
- Real time open source reconnaissance against employees, vendors, and infrastructure

Impact

Business email compromise and CEO fraud wire transfers. Ransomware enabled by faster exploit weaponization. Account takeover and MFA bypass through deepfake voice. Large scale credential phishing and vendor impersonation.

Adversaries Using Our AI Against Us

- Prompt injection and jailbreak of customer facing or internal AI assistants
- Sensitive data exfiltration through unsanctioned AI tools (shadow AI) and overbroad copilot permissions
- Model and training data poisoning that alters outputs at scale
- Compromise of autonomous agents producing lateral movement inside the enterprise

Impact

Sensitive data and trade secret exfiltration via shadow AI. Prompt injection driving unauthorized actions and data disclosure. Supply chain compromise through poisoned models. Agent hijacking enabling lateral movement and privilege escalation.

Note: prior version referenced Mythos and GPT 5.4 as illustrative model and threat actor examples. Refresh with current threat intelligence before external distribution.

Mythos and What It Means for Security

Anthropic's vulnerability-discovery model is now public, and it changes how fast attackers can move.

BOTTOM LINE Your security program needs to move faster across the board — patching, detection, response, vendor oversight, and staffing.

01 What is Mythos?

- Anthropic's AI model shared with vetted security researchers to help find software vulnerabilities.
- It is real, public, and the first of several such tools — OpenAI has shared GPT 5.4 Cyber on similar terms.
- Defenders use it to find bugs faster. Attackers use the same class of tools to write working exploits faster.

02 What changes for IT

- The window between a flaw being announced and being attacked is shrinking from weeks to days.
- "Patch only the high-severity ones" no longer works — NIST stopped fully analyzing most new CVEs in April 2026.
- Priority is shifting to CISA's Known Exploited Vulnerabilities list — the bugs actually being used right now.

03 Questions worth asking

- How many current vulnerabilities do we have in our environment?
- Are we enriching our data with business context?
- What are our patching SLAs and have we been meeting them?

Sources: NIST NVD program update, April 15, 2026; CISA KEV Catalog and BOD 22-01; Anthropic and OpenAI public communications on Mythos and GPT 5.4 Cyber.

What About the Legal Implications of AI?

- States continue enacting more laws directed to regulate AI
  - Bias, transparency, data usage restrictions, synthetic media
  - Employment, medical, political ads, deep fakes
  - Catastrophic risk
- Legal exposure tied to:
  - Training data
  - Automated decision making
  - Not auditing AI in environment, and not sure what AI is doing

How to Address AI Risk: AI Governance Framework

- Do you know what AI is in your environment? And what tools are being used?
- Policies for:
  - Creation (if appropriate) and use of AI
  - Data inputs/outputs
- Risk assessment before deployment
  - Mid-market companies will need to level up to enterprise risk monitoring, especially in vulnerability management
  - Will need application security functions to address AI risk

What happened to the hacker?

He Ran Somewhere….

Cyberattacks: Ransomware/Exfiltration Evolution

- Double/triple extortion
- Companies need to protect hundreds of endpoints, threat actors only need one slightly cracked window
- Attacks are becoming more catastrophic
- Threat actors targeting critical infrastructure, SaaS providers, and supply chain
- Fake publicly posted cyberattacks
- Social engineering
- More SaaS and Cloud Attacks

A Solid Defense Begins With Preparation

- Conduct an asset and data analysis
  - What systems are most important?
  - What data do you have, and where is it? Think about a data diet
- Defense in depth
- Proper implementation of technical tools
- Create a solid incident response plan, and test it
  - Clearly defined incident escalation/de-escalation
  - Who does what – and make sure they know!
  - Communication plan

Supply Chain Risk – Technical

- Reliance on external vendors and service providers continues to increase
  - Cloud providers, Saas tools, IT support, contractors
  - Increased software dependencies
  - Trusted access
  - Misconfigurations remain key issue
  - APIs – primary attack vector in modern apps

Supply Chain Risk – Legal

- Contractual concerns
  - Legacy contracts – or no contracts
  - Limitations of liability very limited
  - Not clear who is responsible for what
  - No requirement to provide information or communicate if a cyberattack occurs
  - No insurance
  - Don’t comply with current cybersecurity and privacy laws

Supply Chain Risk Mitigation

- Contracts are important!
  - Review the cybersecurity representations and warranties – what is the vendor responsible for? What are you responsible for?
  - Limitation of liability, indemnification clauses important
  - Adequate cyber insurance
  - Audit rights
- Contract alignment with real-world risk

Supply Chain Risk Mitigation

- Practical Strategies: Third-Party Risk Management
  - Limited access
  - Continuous monitoring vs. one-time assessments
  - External attack monitoring
  - Certifications versus auditing controls

Ever Increasing Legal and Regulatory Requirements

- Expanding US and Global Privacy and Cybersecurity Requirements
  - Patchwork complexity
    - US state laws (CA, CO, TX, AL as of April 2026)
      - Various industries and sectors – AI, healthcare, employment, critical infrastructure, etc)
    - EU GDPR Evolution
    - New regimes in Asia and Middle East
- Impact Assessments – companies that have the best privacy and cybersecurity hygiene are conducting privacy and cybersecurity assessments.
  - Real dollar impacts to having poor privacy hygiene

Legal and Regulatory Requirements

Explosion of state privacy laws:

- By 2026, 20 states have comprehensive privacy laws
- More coming in 2026, plus amendments to current laws
- Trends include
    - Stronger consumer rights (access, delete, correct data)
    - Expansion of opt-out mechanisms and data broker rules

Laws are becoming more targeted:

- Children and teens
- Health and sensitive data

More enforcement actions

Mandatory Disclosure & Reporting Requirements

- Shortened breach notification timelines
  - Contractual – immediately or promptly
  - US – 14 – 30 days
  - GDPR – 72 hours
- Increased reporting requirements
- SEC disclosure requirements
  - Material cybersecurity incidents
  - Board oversight required

Executive & Board Accountability

- Director's fiduciary duties now include cyber and privacy oversight
- Liability risks increasing:
  - Shareholder lawsuits
  - Regulatory enforcement actions
- General Counsel and CISO may have to sign attestations as to compliance
- Practical advice – move beyond dashboards, reframe as a business risk
  - Not – patch compliance at 87%
  - But – critical vulnerabilities identified in payment process system, creates potential $XX revenue disruption
  - Look at financial exposure, operational disruption risk, regulatory impact

How Do Organizations Prepare?

- Create good privacy and cyber hygiene now
  - Solid, effective, ACTIONABLE policies and procedures
  - Data minimization across Cloud, SaaS, Vendors, internal systems – if you don't need it, delete it
  - Classify data and apply appropriate protections
  - Supply chain management is key
  - Appropriate contracting
- Audit AI in your environment, develop and train on policies (continuous training)
- Develop and test Incident Response Plan, and consider catastrophic risk

Questions?

Melissa Ventrone
mventrone@clarkhill.com

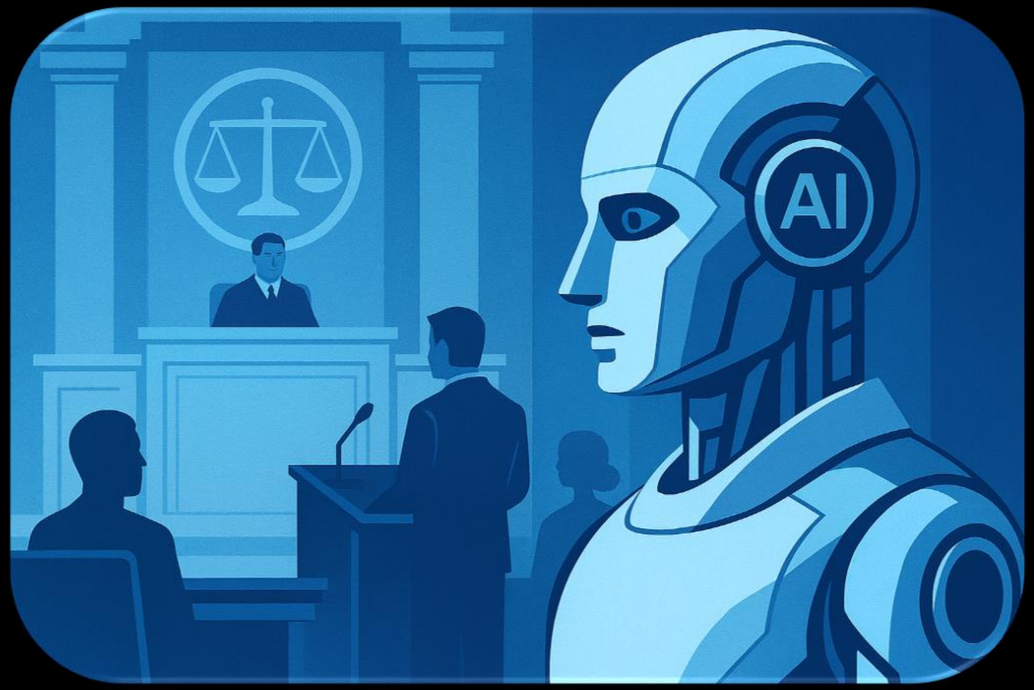
Michael Chada
mchada@enduir.com

Legal Disclaimer
This document is not intended to give legal advice. It is comprised of general information. Employers facing specific issues should seek the assistance of an attorney.

We will resume at 9:40 a.m.

10 Minute Break

Artificial Intelligence Meets the Courtroom: Emerging Risks and Trends in Modern Litigation



2026 Clark Hill Data Privacy and Cybersecurity Law Summit
April 28, 2026 | Chicago, IL

Key Contacts

24/7 Breach Hotline at 877.912.9470 or breachresponse@clarkhill.com

Chad Love, Director of IG360 Discovery Services
+1 214.326.1002
clove@clarkhill.com

Peter Berk, Senior Attorney
+1 312.701.6870
pberk@clarkhill.com

Madison Shepley, Senior Attorney
+1 312.360.5021
mshepley@clarkhill.com

April 2026

INTRODUCTION & ETHICS

SECTION I

Introduction to AI Litigation

Why This Matters Now

- AI increasingly appears:
  - As a fact (what happened)
  - As a tool (how cases are litigated)
- Courts, regulators, and litigants are reacting in real time

Ethical Rules: Competence

Model Rule 1.1

- Duty of competence includes technological competence

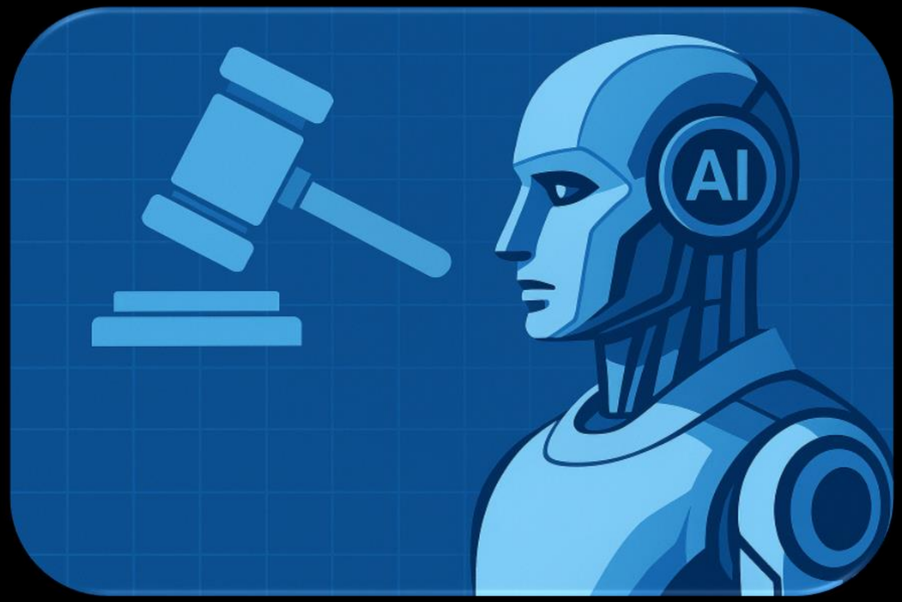
Model Rule 1.6

- Duty of Confidentiality/Privilege issues

Model Rule 3.3

- Duty of Candor towards the tribunal (hallucination issue)

AI BEING LITIGATED



SECTION II

AI as the Defendant

- **Emerging Claim Categories**
  - Privacy
  - Discrimination
  - Specialized statutes
  - Agentic AI

Privacy Claims: Core Statutes

- California Invasion of Privacy Act (CIPA)
- Electronic Communications Privacy Act (ECPA)
- Biometric Information Privacy Act (BIPA)

Discrimination Claims

- **Employment & Housing**
  - Illinois Human Rights Act (AI amendment)
  - Federal Civil Rights statutes
- **Key Theory**
  - No protected class input
  - Bias learned from training data

Agentic AI Litigation

- **Cases to Watch**
  - *Mobley v. Workday*
  - *Amazon v. Perplexity*
- **Takeaway**
  - Less human oversight = higher litigation exposure

AI IN CASE PLANNING

SECTION III

AI For Legal Research

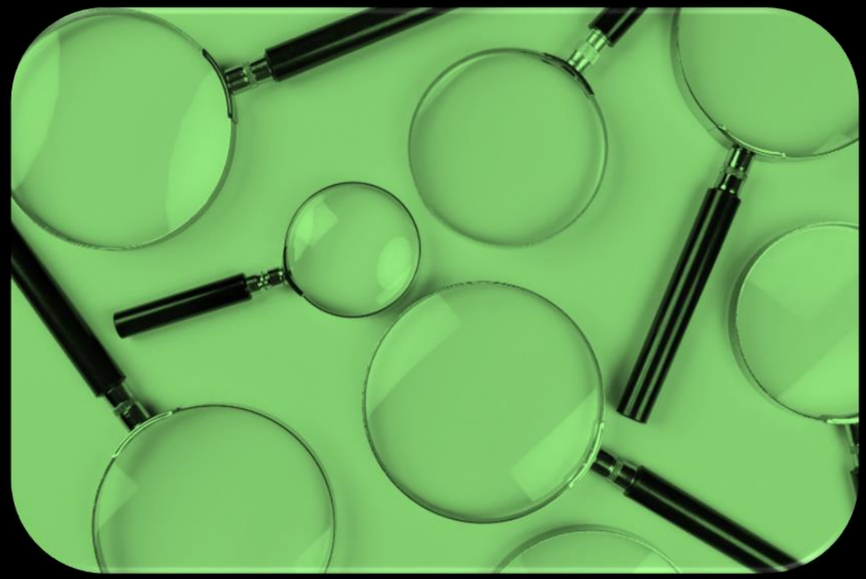
- **Benefits**
  - Speed
  - Issue spotting
- **Risks**
  - Hallucinated cases
  - Fabricated quotations

Hallucination Case Law

- **Examples**
  - *Mata v. Avianca* — $5,000 sanction
  - *Williams v. Chicago Board of Education* — ND Ill.
- **Growing Database**
  - 1,200+ documented incidents

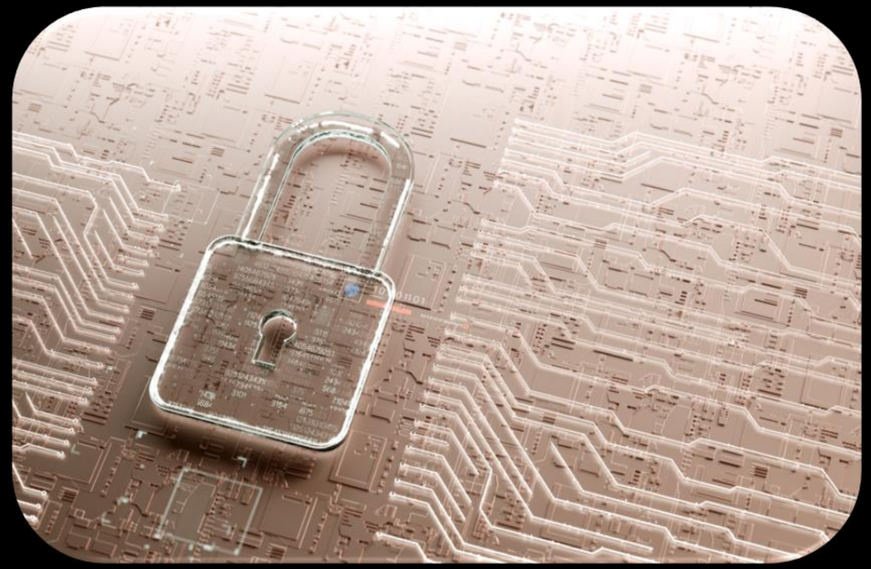
Duty of Candor Revisited

- Rule 3.3 implications
- Rule 11 still applies
- AI ≠ reasonable inquiry by default

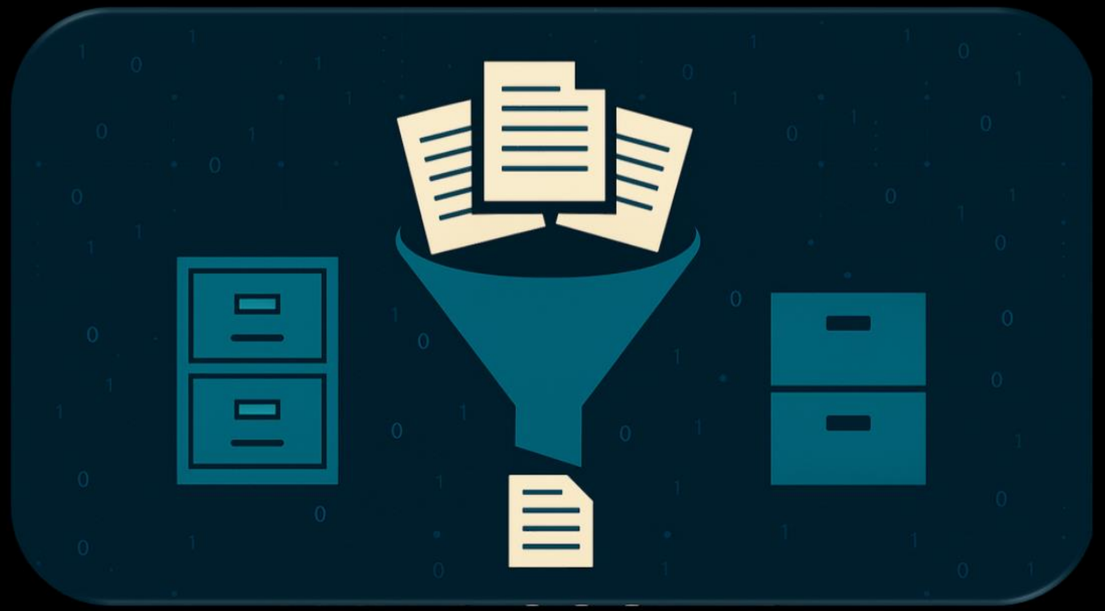


Strategy & Privilege Risks

- Prompt engineering as discoverable material
- Public models and waiver concerns
- *Heppner* implications revisited



AI IN DISCOVERY



SECTION IV

Seeking AI Materials

- **Discovery Targets**
  - Prompts
  - Outputs
  - Policies governing AI use
  - Training data / vendors

Framing Discovery Requests

- **Key Question**
  - Who “created” the content?
  - Does the tool retain data?
  - Is AI use governed by policy?

DOCUMENT REVIEW A LOWER RISK USE CASE FOR GAI

Using GAI to generate Court Facing Documents. **HIGHER RISK**

VS

Using GAI to locate relevant documents **MUCH LOWER RISK**

However……

COURTS' FOCUS SHIFTS TO EXPOSURE OF CONFIDENTIAL/PRIVILEGED INFORMATION

***United States v. Heppner*, Southern District of New York**

- Client use of the AI platform Claude to generate documents for legal consultation did not merit privilege protection.

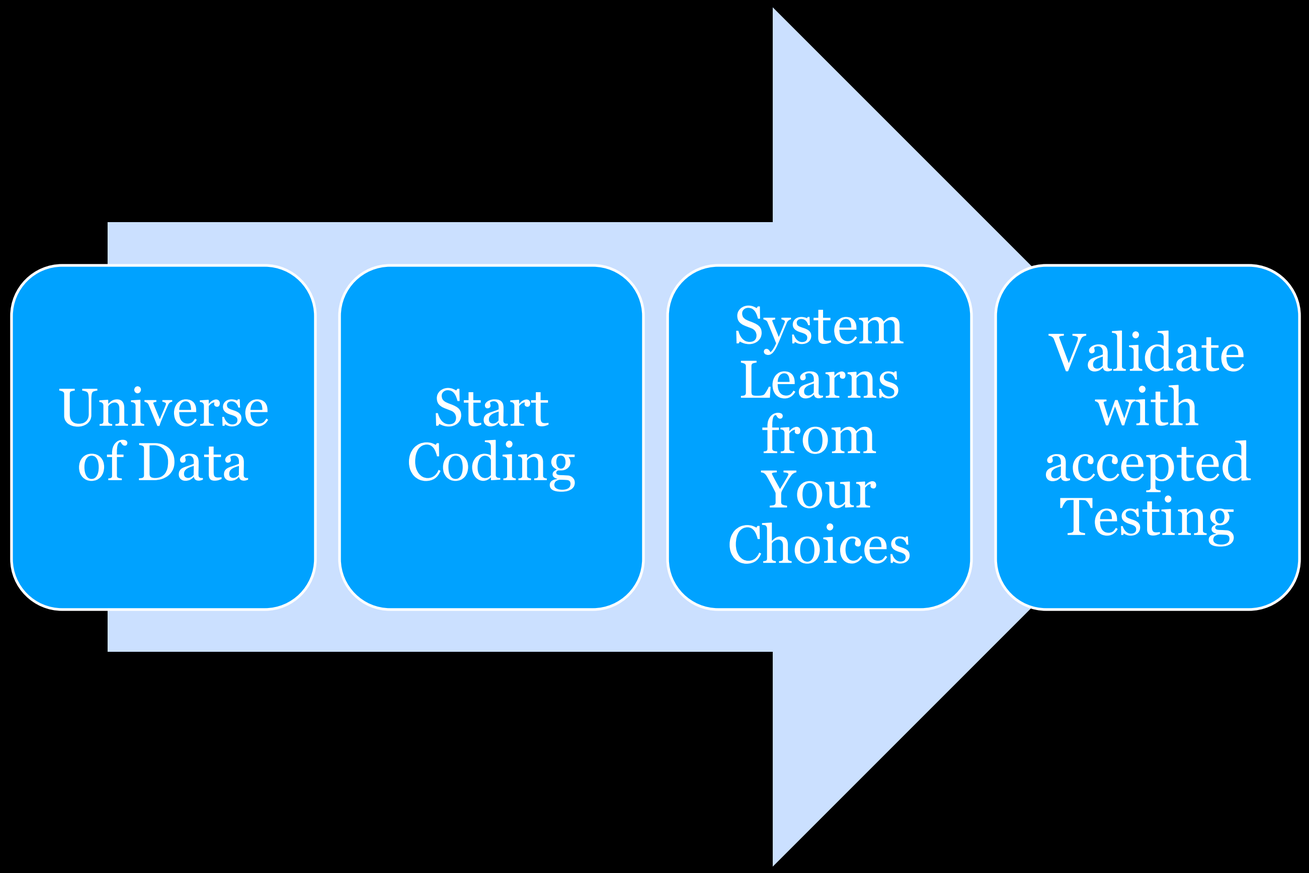
***Warner v. Gilbarco*, Eastern District of Michigan**

- ChatGPT and other generative AI programs are tools, not persons.
- Work product waiver requires disclosure to an adversary.

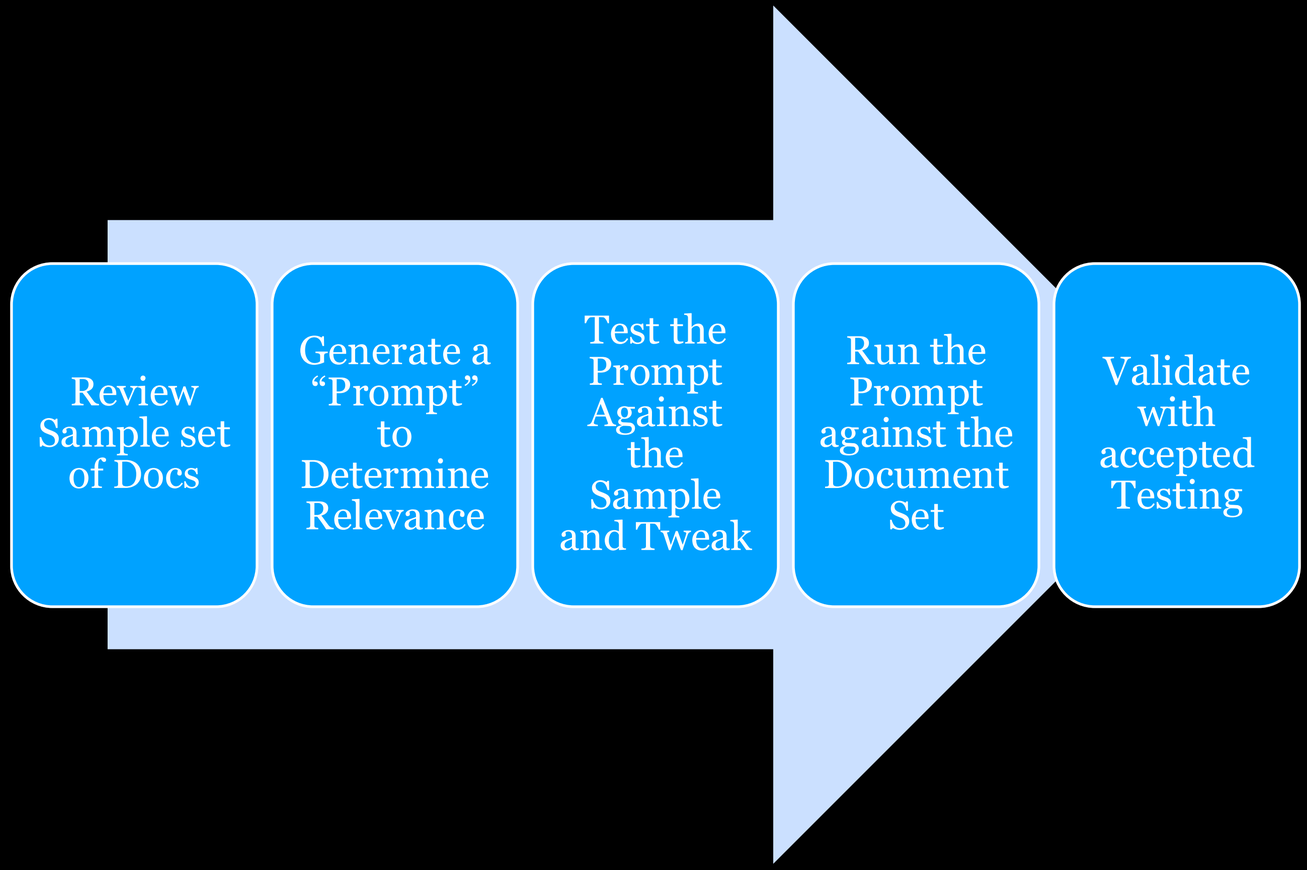
***Morgan v. V2X*, District of Colorado**

- Contractual safeguards must be in place with GAI tool provider.
- No training on inputs
- No third-party disclosure
- Must allow deletion of data

AI IN THE BEGINNING – TAR
TEACHING THE SYSTEM WITH YOUR CHOICES



GAI FOR DOCUMENT REVIEW
"PROMPTING" THE SYSTEM



VARIOUS USE CASES

Prompts can be developed for:

- Relevance
- Privilege
- Key Docs
- Issues
- Confidential Business Information

NATURAL LANGUAGE SEARCHING

Ask the system anything about your document set.

NO RISK USE CASES FOR GENERATIVE AI

- Incoming Document Production
- For prioritizing our client documents.
  Even if you want to look at them all
- For doing document summaries.

AI IN THE COURTROOM

SECTION V

AI Generated Evidence

- **Key Concerns**
  - Authenticity
  - Foundation
  - Reliability

Existing vs. Proposed Rules

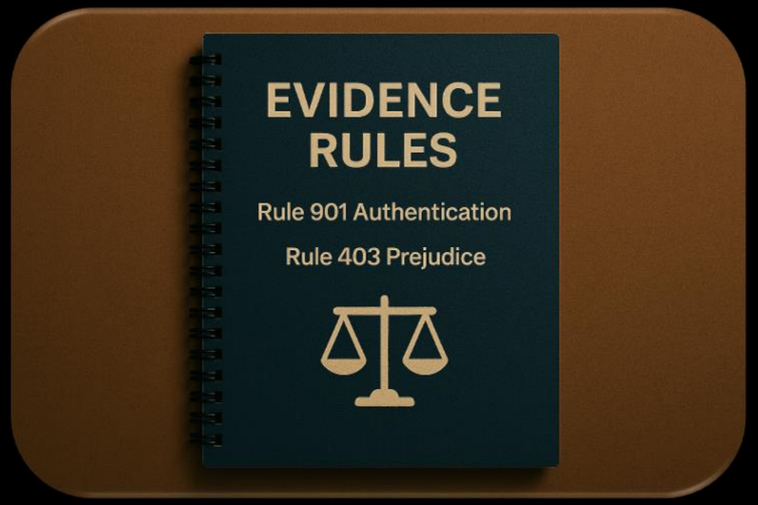
Proposed FRE 707

Machine-Generated Evidence

- Subject to Rule 702(a)–(d)
- Expert-quality reliability required
- Not effective until Dec. 1, 2027 (projected)

Existing Evidence Rules

- Rule 901 — Authentication
- Rule 403 — Prejudice
- Implicit bias in AI outputs



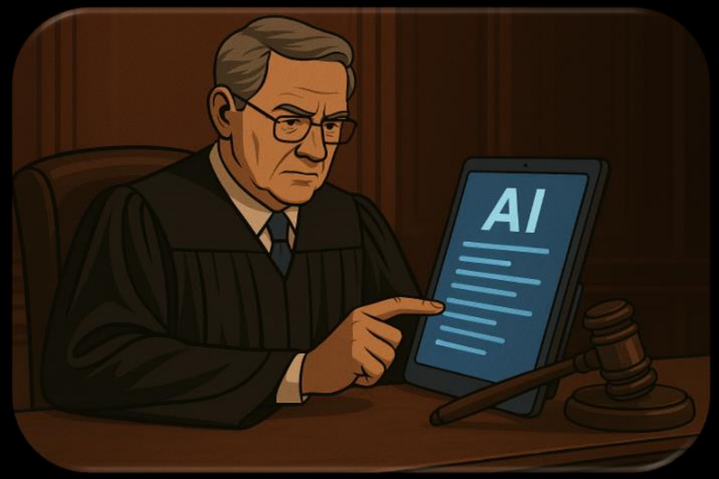
Judicial Use of AI

Recent Study: Anika Jaitley, Daniel Linn Jr., Honorable Xavier Rodriguez, V.S. Subrahmanian and Siyu Tao "*Artificial Intelligence in Federal Courts: A Random Sample Survey of Judges*" 27 SEDONA CONF J. _____

- Random sample of 502 Federal Judges (Bankruptcy, Magistrate, District court and Appellate court)

Survey Highlights

- 60% of judges use at least one AI tool
- Only 22% use regularly
- 38% report no use at all



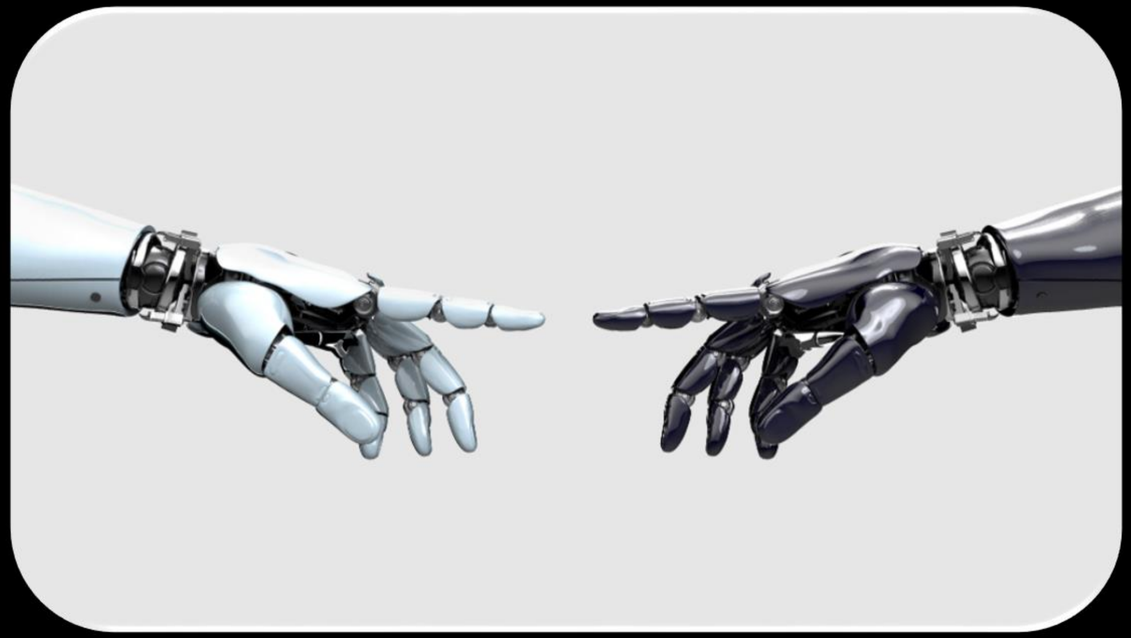
Judicial Concerns (Quotes)

- Themes:
  - Lack of training
  - Hallucinations
  - Need for guardrails
  - Caseload realities

Juries & AI

- Risk jurors believe AI demonstrations are “real”
- States exploring jury instructions
- Heightened Rule 403 concerns

LOOKING FORWARD



SECTION VI

Key Takeaways

- AI is now embedded in litigation
- Ethical, procedural, and evidentiary risks are converging
- Courts expect transparency + competence

Call to Action:

- Understand how AI is being used — by everyone
- Update policies now
- Prepare clients before litigation starts

Questions?

Peter Berk
pberk@clarkhill.com

Chad Love
clove@clarkhill.com

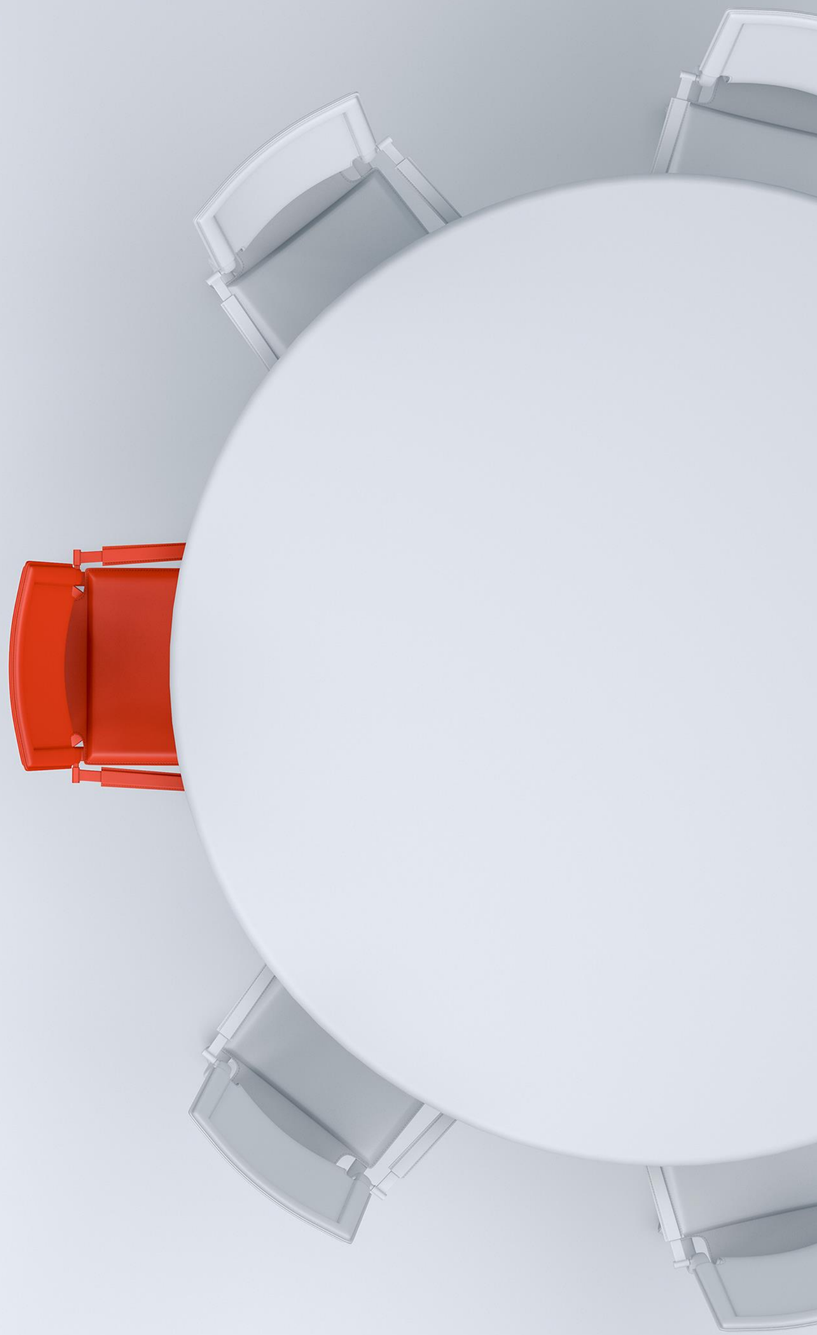
Madison Shepley
mshepley@clarkhill.com

We will resume at 10:50 a.m.

10 Minute Break

Clark Hill

Roundtable Discussion



Thank You

Please complete survey and sign out for CLE

Legal Disclaimer

The views and opinions expressed in this material represent the view of the authors and not necessarily the official view of Clark Hill PLC. Nothing in this presentation constitutes professional legal advice nor is it intended to be a substitute for professional legal advice.

Clark Hill