



AI 2035: The Legal Profession and the Judiciary in the Age of Artificial Intelligence

Confidentiality in the Age of AI: When Client Data Becomes Training Data

Examine the confidentiality risks that arise when client data interacts with AI systems, including concerns about data retention, model training, and third-party tool usage. You will gain practical guidance on safeguarding sensitive information while leveraging AI in transactional workflows.



Michael R. Booden, Senior Technology Counsel, HUB International Ltd.

Michael Booden is Senior Technology Counsel at HUB International Ltd., supporting global organizations across a wide range of legal and operational issues. Michael focuses on commercial transactions, technology agreements, and compliance initiatives. He is known for delivering practical, business-focused legal advice. Michael also advises on AI, data privacy, and internal investigations.



Peter Hegel, Counsel, Perkins Coie

Peter Hegel is of counsel at Perkins Coie. Peter counsels clients on protection of personally identifiable information (PII) and infrastructure, as well as other issues arising under domestic data security and privacy laws and regulations, including the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA).



Nicholas Ustaski, Associate, Dykema

Nicholas Ustaski represents employers in complex labor and employment matters at Dykema in Chicago. Nicholas advises on compliance, corporate transactions, and litigation defense. He has extensive experience in multi-state employment law and workplace policy development. Nicholas focuses on helping clients mitigate risk and avoid litigation. He is also committed to pro bono service and community engagement.



Moderator: Jennifer Dickey, Associate, Dykema

Jennifer Dickey is an associate in Dykema's Chicago office. She focuses her practice on advising organizations on privacy compliance and regulatory requirements. Jennifer helps businesses navigate complex data privacy frameworks and implement proactive strategies to mitigate risk and ensure operational alignment with evolving laws.

THE CHICAGO BAR ASSOCIATION PRESENTS:

**AI 2035: The Legal Profession and the
Law in the Age of Artificial Intelligence**

Confidentiality in the Age
of AI: When Client Data
Becomes Training Data

May 12, 2026

1:30-3:00 pm



THE
CHICAGO
BAR
ASSOCIATION

Speaker Biographies

Michael Booden is Senior Technology Counsel at Hub International, the fifth-largest insurance brokerage and benefits provider in the world. He negotiates and drafts complex commercial agreements with a focus on technology transactions, represents Hub in commercial disputes, and develops company-wide policies, including Hub's Policy for Using Generative Artificial Intelligence in the Workplace.

For the past thirteen years, Michael has served as an Adjunct Law Professor at The University of Illinois Chicago School of Law. He has written publications that have appeared in the ACC Docket, Chicago Bar Record, and IICLE and has spoken at programs organized by the Associate of Corporate Counsel, the Chicago Bar Association, the Masters Conference, and other organizations.



Speaker Biographies

Peter Hegel counsels clients on protection of personally identifiable information (PII) and infrastructure, as well as other issues arising under domestic data security and privacy laws and regulations, including the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA). Peter has completed several successful secondments, including with a major social networking company, a major online retailer, and a multinational online search engine platform. As such, Peter has extensive experience working closely with in-house legal and compliance departments in delivering pragmatic and timely advice to cross-functional groups across the business.



Speaker Biographies

Nicholas M. Ustaski represents employers of all sizes in a variety of industries on complex employment matters, including experience on hundreds of matters related to complex national and international corporate transactions and in all phases of litigation defense and counseling. His practice primarily consists of, labor and employment due diligence, policy review and revisions, executive management consulting and advisement, mergers and acquisitions and other types of transactions, and employment litigation defense, where Nick's passion for research, writing, and the nuances of labor and employment law shines.



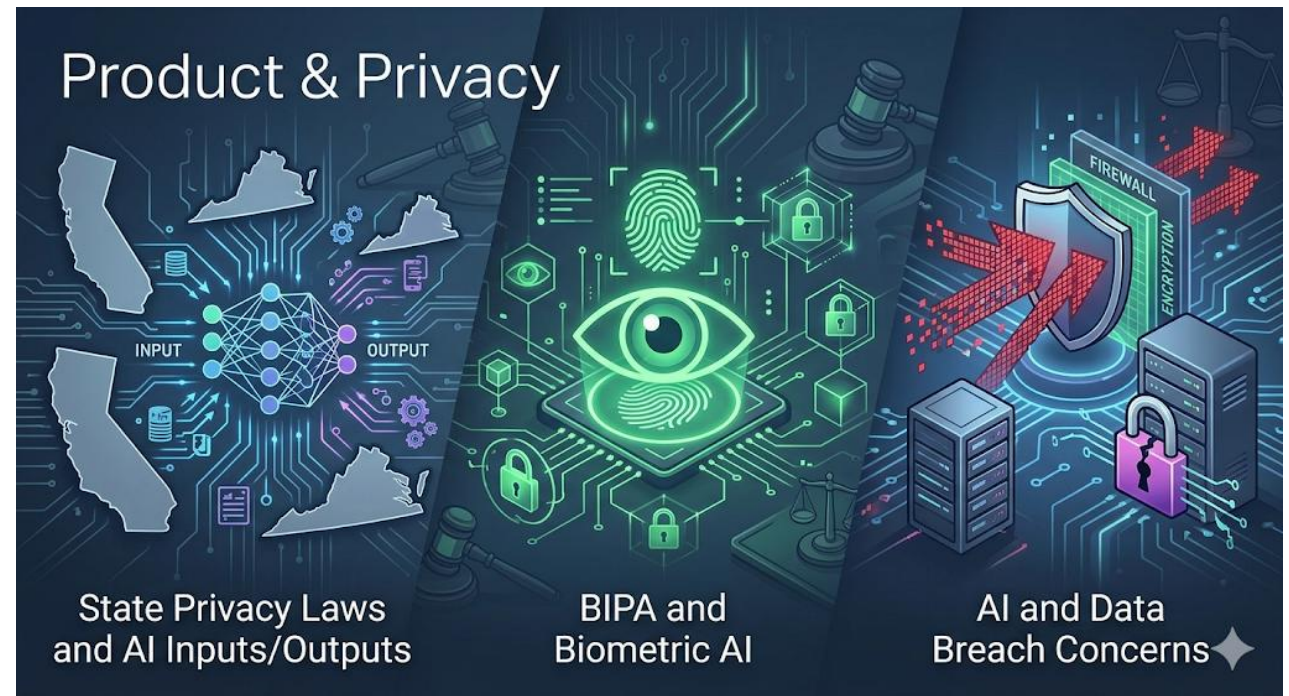
Introduction

- Why This Topic, Why Now?
- AI 101 for Lawyers
- Where AI Already Lives in Your Workflow



Product & Privacy

- State Privacy Laws and AI Inputs/Outputs
- BIPA and Biometric AI
- AI and Data Breach Concerns



AI in the Workplace: Legal Risks & Practical Realities

- The Current Landscape
- Employees Using AI
- Employer Use of AI
- AI Driven Employment Litigation and Transaction Trends
- AI Governance: What Employers Should Be Doing
- Key Takeaways



AI in the Workplace: The Current Landscape

- Widespread adoption of generative AI tools in workforce.
- Dual use: Employees and Employers
- AI integrated into: Drafting, coding, analytics; HR and decision-making tools.
- Key tension: Efficiency vs. control vs. fairness
- Law is evolving slower than technology.
- Companies often don't fully know how employees are using AI



Employee Use of AI: Opportunities & Risks

2. EMPLOYEES USING AI



Opportunities: Increased productivity and efficiency; faster drafting, research, and problem-solving; and augments employee skillsets

Employer Risks: Confidential/proprietary data exposure; inaccurate or fabricated outputs (“hallucinations”); intellectual property ownership concerns; “Shadow AI” use without oversight

Employee Risks: Discipline or termination for misuse; ethical concerns (plagiarism, accuracy); overreliance impacting performance

Best Practices: Clear AI usage policies; training and guardrails; disclosure requirements

Example: Employee pasting client data into ChatGPT. Most risk is unintentional misuse.

Employer Use of AI in Employment Decisions

- **Common Uses:**

- Hiring (resume screening, candidate ranking)
- Productivity monitoring and work assignment
- Performance evaluation
- Discipline and termination decisions

- **Legal Risk Areas:**

- Discrimination and bias (Title VII, ADA, FMLA, ADEA)
- Lack of transparency
- Failure to accommodate disabilities
- State/local AI regulation (notice + audit requirements)

- **Employee Concerns:**

- Lack of due process
- Inability to challenge decisions
- Privacy and surveillance



AI-Driven Employment Litigation

4. LITIGATION & ENFORCEMENT TRENDS

EMERGING CLAIMS

- Disparate impact from AI tools
- Failure to accommodate
- Wage & hour issues from AI tracking
- Wrongful termination based on flawed AI outputs



AGENCY FOCUS

- EEOC
AI bias enforcement
- FTC
Deceptive AI practices
- DOL
Worker monitoring & classification

LITIGATION TRENDS

- Focus on employer and vendor
- Discovery disputes over algorithms
- Increased scrutiny of automated decisions

- **Emerging Claims:**

- Disparate impact from AI hiring tools
- Failure to accommodate in automated systems
- Wage & hour issues tied to AI tracking
- Wrongful termination based on flawed AI outputs

- **Agency Focus:**

- Equal Employment Opportunity Commission (EEOC): AI bias enforcement
- Federal Trade Commission (FTC): deceptive AI practices
- Department of Labor (DOL): worker monitoring and classification

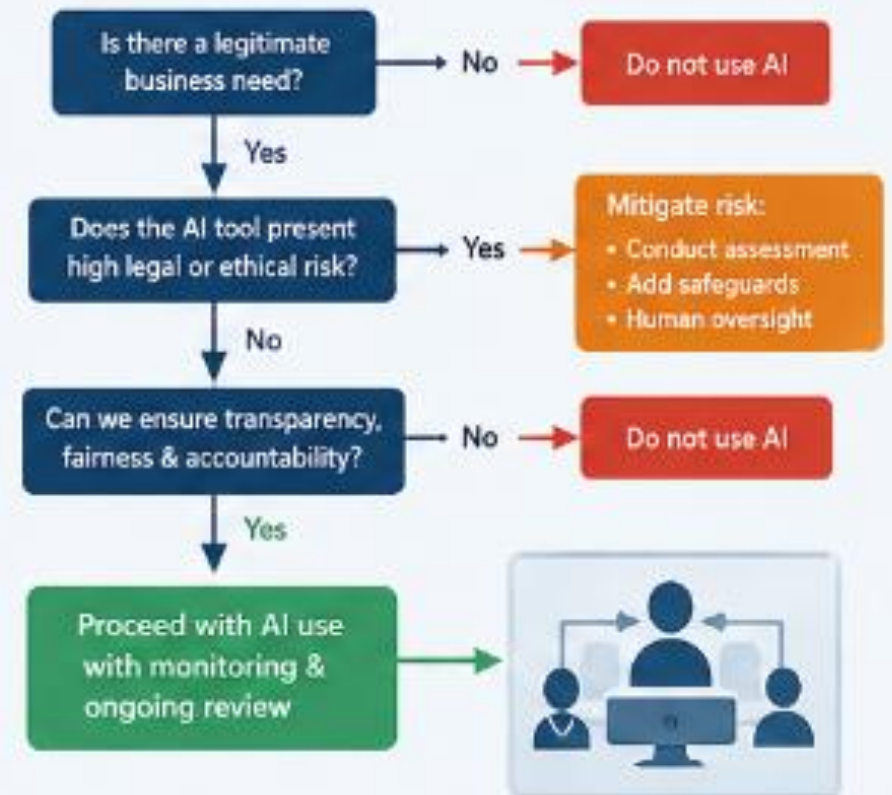
- **Litigation Trends:**

- Focus on both employer and AI vendor
- Discovery disputes over algorithms
- Increased scrutiny of automated decisions

Key Takeaways for AI in Employment

- AI use is already happening—whether you regulate it or not.
- Employee use creates **data and IP risk**.
- Employer use creates **bias and liability risk**.
- Regulators are actively focused on AI.
- Governance, policies, and training are critical.

6. DECISION TREE – SHOULD WE USE AI FOR THIS?



AI Governance: What Employers Should Be Doing

Policy Trends:

- Formal AI usage policies
- Restrictions on unauthorized tools
- Disclosure requirements

Contracting Trends:

- Vendor agreements addressing:
 - Data use and retention
 - Indemnification
 - Bias testing / audit rights

Employment Agreement Updates:

- Expanded confidentiality provisions
- AI-specific IP assignment language
- Acceptable use restrictions

Best Practices:

- Conduct AI risk assessments
- Implement human oversight
- Audit tools regularly
- Train HR and managers

Your Role in Establishing AI Governance

- 2½ years ago, I realized that sometime soon, a significant number of my company's 21,000+ employees were going to want to use AI to help them do their jobs. And we will need an AI Governance Policy to manage this usage.
- On behalf of your clients, attorneys are uniquely positioned to lead AI Governance—not just react to it.
- Hub International is the fifth largest insurance brokerage company in the world. If we were publicly traded, we'd be a Fortune 500 company. We help businesses get insurance that they rely upon for their global operations.
- Our clients trust us with some of their most sensitive data imaginable — NPI, including their strategic goals, and the PII, SPI and PHI of their customers and employees.
 - **This trust must always be respected.**

AI Governance, Confidentiality and Compliance

- With publicly available AI tools proliferating like ChatGPT, it didn't take too much imagination for me to realize that my fellow employees, without guidance, might be tempted to use these AI Tools in serving our customers.
- **Without a policy. Without guardrails.** Without anyone really knowing what Confidential Information was going out the door and how it would affect Hub, our customers and their employees.
- Use of such publicly available AI Tools is also a data breach waiting to happen—with potential regulatory violations and lawsuits as a reward.
- That's why your advice and counsel to corporate clients on establishing appropriate AI governance and compliance policies essential to protect your clients and their Confidential Information.

AI Governance, Confidentiality and Compliance

- These AI governance and compliance obligations all spring from a central source: **What does the law require?** This is fundamentally a question that we are responsible for answering.
- **What advice can we give clients in drafting AI Governance Policies to protect their Confidential Information?**
 - Never put CI, PII, SPI or PHI into an AI Tool not approved by your AI Governance Committee for such usage.
 - Only use AI Tools that your client has licensed, e.g., Claude. In your contracts with these vendors, you need affirmative representations that: 1) your client's **Inputs and Outputs** aren't shared with third parties or used to train the vendor's AI Tools; and 2) these **Inputs and Outputs are your client's Confidential Information.**

Establishing an AI Governance Committee

What's next? A policy is not a governance program.

- AI Governance Committee should include cross-functional ownership: representation from IT, Legal, HR, Compliance, Marketing, Operations — not just lawyers, not just technologists.
- **What is the AI Governance Committee mission? It must be the central authority for:**
 - Selecting which AI Tools your clients will license and make available to their employees.
 - Which categories of information, e.g., PII, SPI and PHI can be used in which AI Tools.
 - Employee training and ongoing compliance with AI governance policies.

AI Usage: Three Things to Know

There are the three things you must know about the usage of AI Tools.

First: It has already affected your corporate clients' relationships with their vendors, customers and outside counsel.

Confidentiality protections of all parties must travel with the data and be memorialized in writing. These can be memorialized in different ways.

- Vendor AI Addendum
- Customer AI Addendum
- Outside Counsel Firm Guidelines in Providing AI Services

AI Governance, Confidentiality, and Compliance

Second: The regulatory landscape is moving fast, and you must keep up.

Colorado. California. Illinois. New York. A regulatory patchwork of laws is already here. Illinois' biometric privacy law has real teeth. You cannot outsource responsibility for compliance with these laws to your IT team.

Third: Policy without culture is just a document.

The training obligation in your AI Governance Policy isn't bureaucratic box-checking. It's the mechanism by which governance becomes behavior.

Mandatory completion of required training. Annual recertification. Retention of training records. A record of relying on progressive discipline when policy violations occur. This all matters because when something goes wrong — **and eventually something will** — your client will need to show regulators, courts, customers and investors that it had an appropriate AI Governance Policy in place and enforced it.

Our Role: Enablement, Not Prohibition

Our job as lawyers is not to eliminate risk — that's impossible. It's to mitigate risk through advice and counsel common-sense governance and effective training.

Your corporate clients should: 1) License secure, enterprise-grade AI tools precisely so they can use AI capably — without exposing them and their respective customers and employees to the wild-west risk of public consumer tools; 2) establish AI Governance Policies that provide appropriate guidance on employee's usage of AI Tools; and 3) establish an AI Governance Committee to ensure compliance with such policies.

Your job is to help them develop these policies to protect their Confidential Information and maintain compliance with applicable laws.

Essential AI Contractual Protections

AI Vendor agreements often don't address the most significant AI-specific risks that your organization will likely face.

Vendor AI Addendum

- **Define Terms:**

- AI and AI Tools: defined broadly so that vendors can't argue that a particular AI feature is not covered.
- Input Data and Output Data: should each be defined be your client's IP and can't be used to train the vendor's LLM.
- Consequential Decision: needs to be defined as they may trigger heightened obligations by state laws (See California and Colorado). Examples: education, employment, financial/lending, housing.
- Algorithmic Discrimination — defined to cover unlawful differential treatment or disparate impact based on protected characteristics addressed in state laws (See Colorado).

Vendor AI Addendum Reps and Warranties

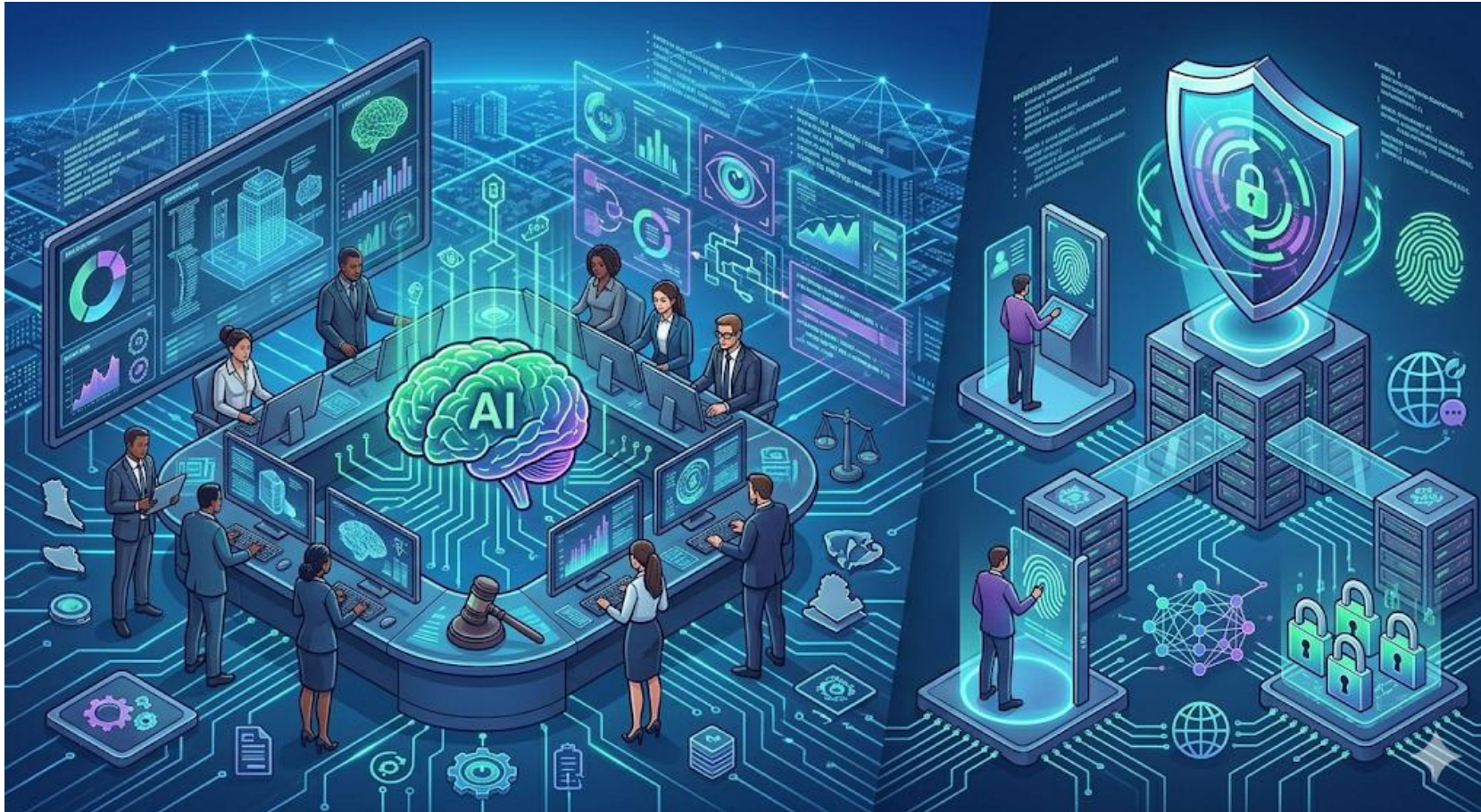
Consequential Decisions. Where the AI Tool is intended to make or is a substantial factor in making, Consequential Decisions, then the Provider shall:

- Provide you the information about the AI Tool sufficient for you to conduct a privacy impact assessment.
- Have a written process in place to monitor for and remedy, at the algorithm level, if necessary, Output Data that discriminates on improper bases.
- Disclose to you any known or reasonably foreseeable risks of Algorithmic Discrimination within ninety (90) days of discovery.

Cybersecurity Requirements. The AI Tool shall operate in compliance with cybersecurity requirements of

- NIST AI Risk Management Framework
- ISO 42001 (AI Management Systems)
- All federal, state and local laws and regulations addressing the use of AI Tools

Hypothetical Scenarios



Audience Q&A



Thank You!



AGENDA FOR “CONFIDENTIALITY IN THE AGE OF AI” PANEL PRESENTATION

Introduction (~10 min)

- Why This Topic, Why Now?
- AI 101 for Lawyers
- Where AI Already Lives in Your Workflow

Product & Privacy (~15 min)

- State Privacy Laws and AI Inputs/Outputs
- BIPA and Biometric AI
- AI and Data Breach Concerns

AI and the Workforce (~20 min)

- AI in the Workplace: Legal Risks & Practical Realities
- AI in the Workplace: The Current Landscape
- Employees Using AI
- Employer Use of AI in Employment Decisions
- AI-Driven Employment Litigation
- AI Governance: What Employers Should Be Doing

Vendors & Contracting (~20 min)

- AI Governance: What Employees Should Be Doing
- Your Role in Establishing AI Governance
- AI Governance, Confidentiality and Compliance
- Establishing An AI Governance Committee
- AI Usage: Three Things to Know
- AI Governance, Confidentiality and Compliance
- Essential AI Contractual Provisions
- Vendor AI Addendum Reps and Warranties

Hypothetical Scenarios (~15 min)

Audience Q&A (~10 min)