Hilgers PLLC

From Experimentation to Adoption: The Legal Side of Generative AI

Prepared for AGMA Winter Conference

FEBRUARY 2026

Speakers

Carly Abramson Kliger

Partner

561-485-1325

ckligler@hilgerslaw.com

Sarah Resczenko

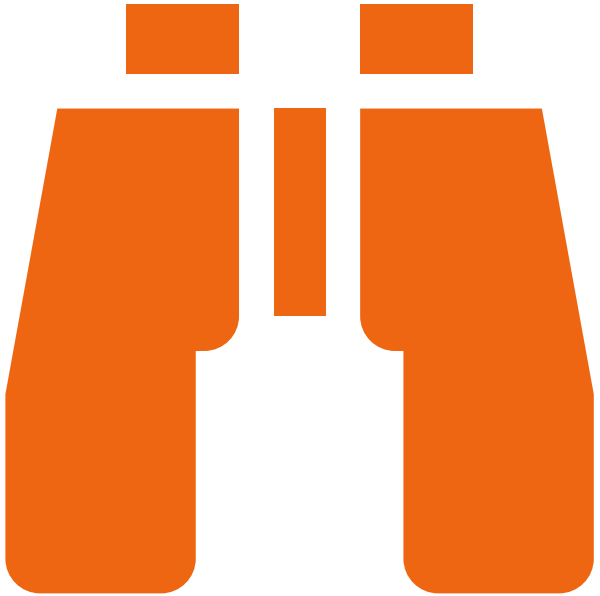
Senior Counsel

352-266-3794

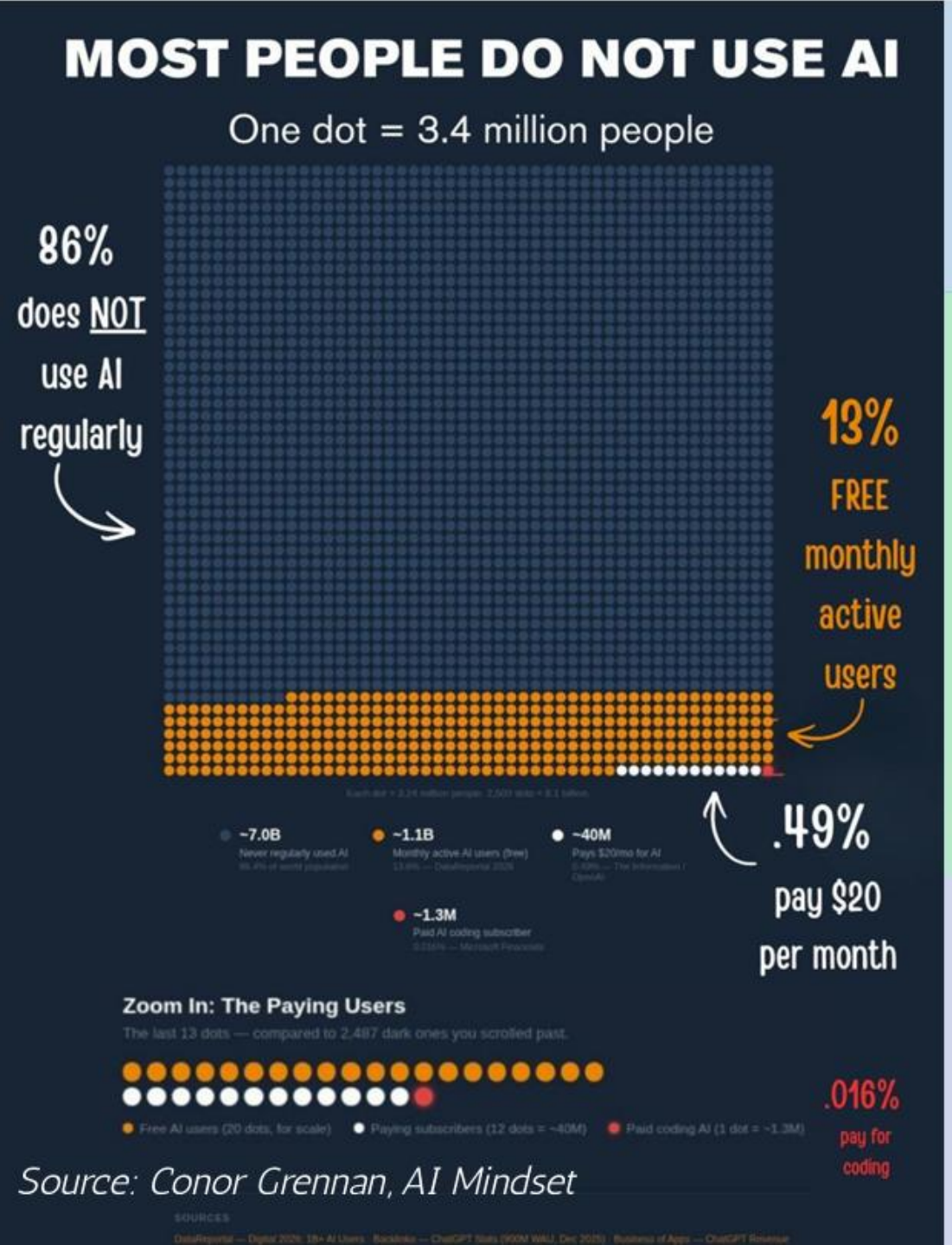
sresczenko@hilgerslaw.com

Agenda

- The State of AI Adoption
- Regulatory Landscape Highlights
- Case Law Developments
- Plaintiffs Bar Use Case Examples
- Final Thoughts - Takeaways



Overview: Current State of AI Adoption



Approximately half of all employees are using Shadow AI (i.e. non-company issued AI tools)

(Software AG October 2024 Study)

95%

of AI pilots within large companies are failing

(The GenAI Divide: State of AI in Business 2025, MIT NANDA Initiative)

- **Approximately 88% of companies report using AI in their organization**
- **44% of surveyed employees feel using AI is "making them dumber."**

Harvard Business Review (2026) – Why AI Adoption Stalls

72%

of executives say their organizations have "integrated and scaled AI" in most or all initiatives...

...yet only a third of companies have in place the proper protocols.

(EY Survey: AI adoption, June 2025)

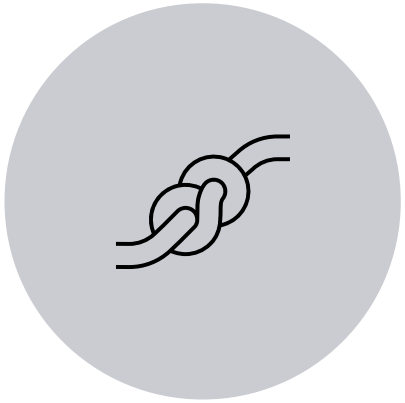
A U.S.-based survey of 1,000 enterprise employees revealed 57% had entered sensitive or confidential company data into public AI tools such as ChatGPT or Google Gemini.

- **31% entered personally identifying details (names, emails, phone numbers)**
- **29% disclosed project-specific or product design information**
- **21% submitted customer-related data**

(TELUS Digital Survey, 2025)

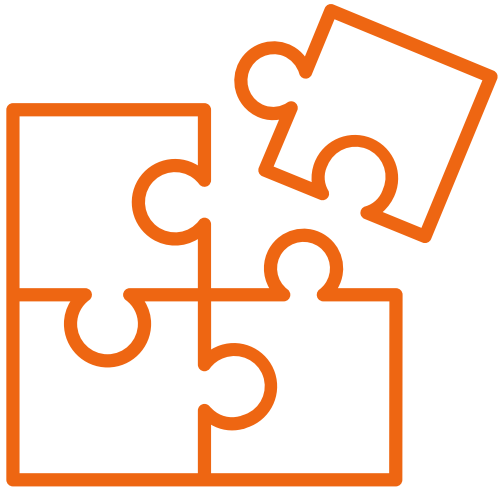
Regulatory Landscape Highlights

EU AI ACT



UNITED STATES
(STATE & FEDERAL)

Jurisdiction	Regulatory Intensity	Governance Model	Business Impact
U.S. – Colorado (AI Act)	🟥 Medium–High	"High-risk" AI governance; anti-discrimination focus	Impact assessments; reasonable care; consumer disclosures
U.S. – New York (RAISE Act)	🟥 Medium–High	Frontier model safety + incident reporting	Model-level safety documentation; reporting obligations
U.S. – California	🟥 Medium	Transparency + safety-oriented; sector overlays	Disclosure and compliance tracking; evolving requirements
U.S. – Other States (Patchwork)	🟧 Emerging	Targeted (hiring tools, deepfakes, elections, child safety)	Multi-state compliance management; monitoring burden
U.S. – Federal (No omnibus AI statute)	🟧 Emerging / Unsettled	Agency enforcement under existing laws; executive policy; potential preemption tension	Litigation + regulatory risk via existing statutes; uncertainty over state-law durability



Litigation Precedents

Emerging Case Law Precedent

- **In Re: OpenAI, Inc. Copyright Infringement Litigation** (1:25-md-03143) District Court, S.D. New York
- **United States v. Heppner,** No. 25-cr-00503-JSR (S.D.N.Y. Feb. 6, 2026), Dkt. No. 22.
- **In re Otter.AI Privacy Litigation,** No. 5:25-cv-06911, District Court, N.D. California

Plaintiffs Gen AI Lab

Faster Drafting: Demand Letters, Complaints, Discovery Requests

- Law Firms use LLMs trained on prior complaints, demand packages, and discovery templates to generate filings in minutes
- GenAI can adapt templates to multiple jurisdictions and fact patterns, accelerating serial filings (ADA, privacy, product defect, wage/hour)
- Issues:
  - Dramatically lowers the marginal cost of filing → more speculative suits and larger volume of demand letters
  - Demands look “polished” and cite relevant authority even when underlying investigation is thin
  - Accelerates early-stage litigation pressure

Damages Modeling Based on Prior Verdicts/Settlements (LLM Summarization)

- Runing verdict/settlement databases through LLMs to generate damages ranges, comp ratios, and jurisdictional patterns
- Generate automated demand packages with damages calculations using structured and unstructured personal injury data
- Issues:
  - Makes demands appear “data-driven”, raising negotiation stakes early
  - Helps plaintiffs’ firms triage cases more intelligently → they focus on high-value SKUs, known injury types, or repeat fact patterns
  - Increases pressure for early settlement before discovery

Faster Issue Spotting

- Plaintiffs use AI-assisted review for intake records, prior complaints, public filings, policy documents, and your own website or store documentation
- Tools allow mass ingestion and tagging of corporate policies, product manuals, disclaimers, warranties, and social media outputs
- Issues:
  - Plaintiffs can find inconsistencies in your terms, policies, or marketing faster (e.g., warranty language v. product performance; loyalty program disclosures v. practice)
  - Reduces the cost of “fishing expeditions” that defense counsel would normally defeat early

Medical Records / Incident Report Summarization

- GenAI extracts injury descriptions, timeline of care, mechanism of injury, and treatment gaps from medical records or internal incident reports.
- Enables plaintiffs to instantly produce polished PI chronologies and “liability narratives.”
- Issues:
  - Historically labor-intensive step → now plaintiffs can rapidly convert any incident into a litigable claim
  - Higher demand quality → more pressure settlements
  - Retailers with high guest-incident volume see more “matured” claims early

Data Aggregators + Advanced AI Analytics

- Plaintiff firms contract with data brokers or use public scraping to gather product reviews, warranty claims, returns data, job postings, accessibility features, etc.
- Then run LLMs to spot statistical patterns, “red flag clusters,” or potential class theories (pricing, accessibility, defect, privacy)
- Issues:
  - AI lowers the cost of identifying class cohesion and numerosity
  - Enables rapid product-defect theory generation based on Amazon/Home Depot/Lowes reviews, Reddit, YouTube, TikTok “how-to fails,” etc.
  - Heightened risk for any retailer with high-volume SKUs

LinkedIn Sharks—AI Scanning for Compliance Gaps

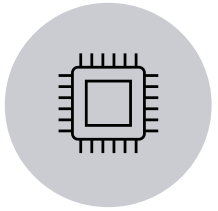
- Plaintiff-oriented “shark” operations use GenAI to scan LinkedIn job posts and company websites to find signals of potential corporate non-compliance
- “Hiring ADA compliance engineer for mobile app remediation” -> suggests accessibility issues
- “Seeking pricing analyst for shelf-tag audit improvements” -> pricing class theories
- No cookies/privacy policy on website -> privacy class action

Mass Advertising for Plaintiff Classes - AI Makes It Cheaper and Faster

- Plaintiff firms contract with data brokers or use public scraping to gather product reviews, warranty claims, returns data, job postings, accessibility features, etc.
- GenAI produces hundreds of ad variants, landing pages, scripts, and A/B tests for plaintiff recruitment
- Deploys micro-targeting on social media to identify potential class members (e.g., people posting reviews or complaints)
- AI models optimize spend → higher conversion, lower cost per claimant
- Issues:
  - Plaintiffs can build class numerosity quickly, making early dismissal harder
  - Higher-volume claims for even small incidents (e.g., minor slip-and-fall, low-value privacy claims)

Final Thoughts - Takeaways

How to Lead with Trusted AI

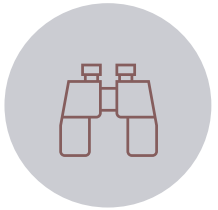


AI Use Inventory: Catalog all AI systems used internally or in customer interfaces & how they integrate with your organization's data map

Prompt & Output Logging: Especially for customer-facing use

Transparency + Consent: Clear disclosures for AI usage in chatbots or personalization

Risk Classification: High/medium/low based on impact and regulatory exposure



Review + Oversight: Central committee or SME to review AI-driven features

Final Thoughts — Leading Through Change with Confidence

- GenAI is not just a technology shift — it's a legal, operational, and ethical inflection point.
- The key to defensibility is intentionality: identify tools, build controls, and update protocols.
- Legal teams must act as strategic partners to guide responsible innovation, not roadblocks.
- Stay proactive: train your teams, evolve your policies, and keep an eye on the legal horizon.
- Those who prepare today will shape the standards of tomorrow.

Legal Risks by GenAI Element

GenAI Element	EU AI Act	US Laws (FTC/State)	APAC Laws
Prompts	High-risk systems must maintain logs; prompts may require human oversight and traceability	May fall under deceptive practice if prompt design is misleading; must avoid privacy violations	Regulations vary: prompts must avoid sensitive question generation; must align with cultural norms (e.g., Singapore, Korea)
Outputs	Outputs must be accurate, non-deceptive; explainability and human-in-the-loop expected for high-risk use	Outputs must not be misleading; false advertising, bias, and hallucinations risk FTC action	Outputs must meet standards for truthfulness and safety; certain markets require AI labeling (China, Korea)
Logs/Metadata	Logging and documentation mandatory for traceability and auditing of high-risk systems	Metadata can be discoverable; must preserve for transparency and explainability if used in decisions	Audit logs and documentation expected for explainability, especially in high-stakes contexts (Singapore's Model AI Governance Framework)
Training Data	Must ensure data quality, diversity, and absence of bias; training data provenance and purpose must be documented	Sensitive or biometric data used in training must comply with CPRA, BIPA, HIPAA where applicable	Consent and fairness requirements for data used in training; China requires source transparency

Extended GenAI Risk Elements

GenAI Element	EU AI Act	US Laws (FTC/State)	APAC Laws
Model Architecture	Requires documentation of model architecture and explainability, especially for high-risk systems	Lack of explainability may pose unfair/deceptive practice risks under FTC Act	Some jurisdictions require explainable AI (e.g., Singapore); black-box models face scrutiny
Fine-tuning Data / Custom Instructions	Fine-tuning must follow data governance and documentation obligations; must ensure quality and relevance	Fine-tuning with consumer data must follow CPRA/GLBA where applicable; risk of sensitive data exposure	Fine-tuning may require consent and data localization; transparency required
Embedded Human Feedback	Human-in-the-loop feedback must be auditable and bias-aware; logs required	Human feedback used to train systems may be considered personal data; requires transparency and consent	Human feedback mechanisms must ensure fairness and prevent discrimination
Third-party Tools/Integrations	Third-party components must be assessed for compliance and risk; liability can extend to integrators	Third-party risk must be disclosed in privacy notices; may be subject to contractual flow-downs	Vendor due diligence and cross-border transfer rules apply (e.g., Japan, China, Singapore)
Deployment Environment (On-prem vs SaaS)	Cloud vs. local impacts data sovereignty and risk classification; local processing may be preferred	Cloud deployments must align with security standards and contractual obligations under HIPAA/CPRA	Data residency and sovereignty rules affect SaaS deployments; must meet local security requirements
Retention Policy / Lifecycle Management	Retention must align with purpose limitation and storage minimization under GDPR	FTC and state laws require that data is retained only as long as necessary for the stated purpose	Lifecycle management obligations include timely deletion and defined retention limits