MCLE LA-LAW-PALOOZA

Smart AI Governance in 2026

ACC – San Diego

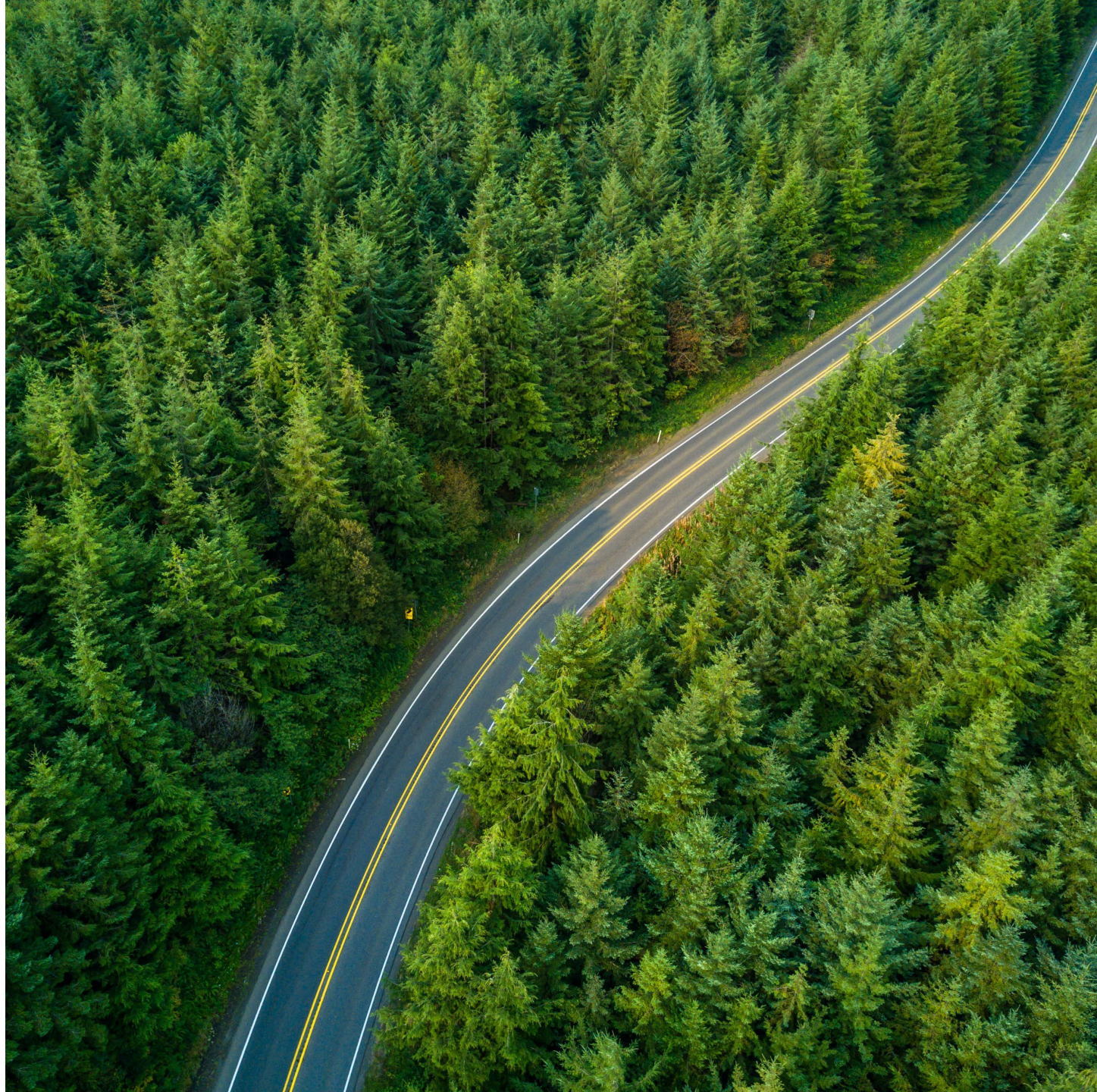
Peter Stockburger
Partner
Foley & Lardner LLP
858.847.6715
peter.stockburger@foley.com

Mary Hardy
Senior Corporate Counsel
Open Source, Standards
and Open Machine Learning
Microsoft Corporation

FOLEY
FOLEY & LARDNER LLP

Roadmap

- ✓ Where AI is heading
- ✓ Global legal landscape
- ✓ Building smart governance in 2026



FOLEY

FOLEY & LARDNER LLP

CONFIDENTIAL

Where AI is heading

AI Definition

An engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments.

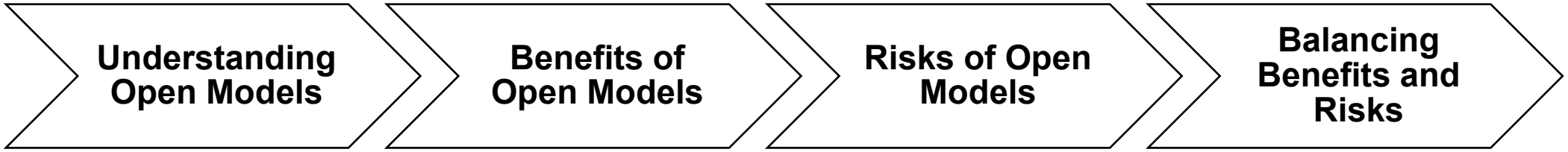
- California Government Code § 11546.45.5(a)(1)
- Colorado AI Act
- Texas Responsible AI Governance Act
- 15 USC § 9401
- EU AI Act
- South Korea Basic AI Act

Where AI has been

- **Deterministic**
  - Rules based, predictable outcomes
  - Traditional computing
  - Auditable, transparent, explainable
- **Examples**
  - Rules based spam filters
  - Decision-tree chat bots
  - Scheduling tools
  - Delivering fixed messages without room for error
  - Knowledge-based filters

- **Probablistic**
  - Predictions from data
  - Machine learning
    - Deep learning
    - Generative (transformer architecture)
      - Large language models (Chat GPT, Gemini, Claude)
      - Large vision models (Sora, Midjourney, Firefly)
      - Large world models (DeepMind Genie, NVIDIA Cosmos, Meta V-JEPA)

Open Models: Benefits and Risks



FOLEY
FOLEY & LARDNER LLP

Where AI is working

Enterprise Workflows

- **Knowledge work automation**. Policy search, knowledge portals, repositories. Legal AI on the rise.
- **Operations workflows**. Customer support automation, dispute processing, legal workflows, accounting, and marketing.
- **Sales enablement**. Call transcripts, structured insight extraction, CRM updating.
- **Coding and software development**. Claude code is enhancing productivity at scale.
- **HR**. Job applicant scanning, employment mobility.

Products & Services

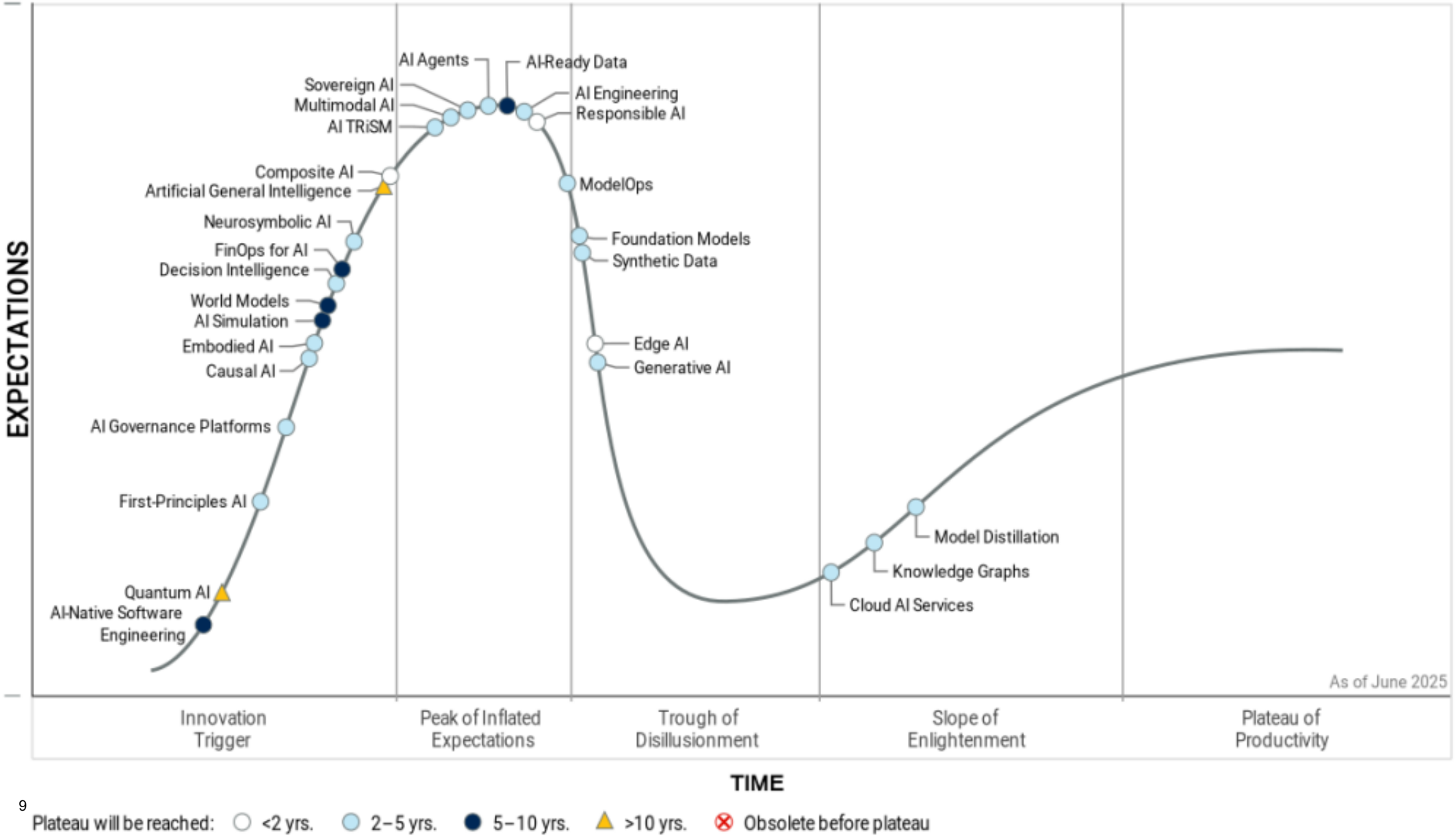
- Conversational interfaces replacing traditional UX.
- Embedded generative output.
- AI enabled software solutions.
- Intelligent automation of customer tasks.
- Real-time insight extraction and decision support.
- Will AI eat all of software?

Agentic AI & Next Level AI

- **What is agentic AI?**
- **Shift from tool-based AI to autonomous decision loops**. Agentic AI systems execute multi-step workflows, introducing delegated authority and audibility challenges.
- **Employee challenge**. Asking for tool access. Building their own agents with OpenClaw / Claude Code / Copilot Studio.
- **Emergent behavior & orchestration risk**. Agentic systems rely on tool-use, API integrations, memory layers, and multi-agent coordination. Emergent or unintended outputs that were not foreseeable during design. Security risks multiply.
- **Liability and agency law tension**. The law of agency and oversight will become tested.

FOLEY
FOLEY & LARDNER LLP

Hype Cycle for Artificial Intelligence, 2025



CONFIDENTIAL

Global AI Legal Landscape

Global AI Landscape

- **Global consensus on the need to regulate AI**. No global consensus on how.
- **Risk-based regulation**. Examples include the EU AI Act, South Korea Basic AI Act, California ADMT regulations, Colorado AI Act.
- **Light-touch / principles based**. Examples include the US federal, Japan, Singapore, Australia.
- **State-control**. Jurisdictions like China are leading the way.

EU

- EU AI Act entered into force on August 1, 2024 and will take effect August 1, 2026.
- Applies extraterritorially to providers, distributors, and deployers who have an establishment in the EU, or are outside and place the AI system into the EU market.
- Classifies AI systems into unacceptable, high, limited, and low risk.
- Key compliance requirements include conducting robust diligence for high-risk systems (and registered such systems in an EU database), robust recordkeeping, technical documentation, and providing certain transparency to the public.

FOLEY
FOLEY & LARDNER LLP

South Korea

- Act on the Development of Artificial Intelligence and Establishment of Trust (AI Basic Act).
- Took effect on January 22, 2026.
- Like EU AI Act, provides high-level requirements for transparency and addressing high-risk AI systems. Applies extraterritorially.
- Applies to both developers and providers of AI.
- High risk is AI that significantly impacts human life, safety, or fundamental rights.
- Ministry of Science and Information and Communication Technology (MSIT) will issue enforcement details.

FOLEY
FOLEY & LARDNER LLP

US Federal

- ✓ No federal AI law.
- ✓ US AI Action Plan (2025). Replaced prior administration EO. Focused on promotion of competition and reducing regulatory burden.
- ✓ Preemption of state laws repeatedly brought up in federal legislation. Funds being withheld as a major stick.
- ✓ Executive branch agencies have authority over FTC Act, EEOC, and existing authorities. White House has asked to dial back enforcement.
- ✓ Courts are looking at discriminatory outcomes and misleading claims.

Workday Lawsuit

- Workday is facing a putative class action in the Northern District of California under Title VII, the ADA, and ADEA.
- Plaintiff alleges Workday's models resulted in discriminatory outcomes.
- Federal judge allowed "agency" theory to proceed. Discovery is ongoing.

- **<u>Why this matters</u>**
  - Agency law being expanded under federal law to software vendors powered by AI because some level of decision-making is passed along to the vendor.
  - Significant risk for HR tooling internally.

US States

- Several states are pushing ahead with AI regulation despite federal challenges.
- California has over 20 AI laws, including forthcoming ADMT regulations on high-risk use cases.
- Colorado AI Act is in limbo and will shake out over the spring. Texas AI Act was watered down and only prevents intentional discrimination.
- Employment related laws in NYC, Illinois, and California.
- AGs are warning they will leverage existing authorities. Privacy laws are leading the way. Litigation is focused on privacy and unique theories (e.g., Eightfold).

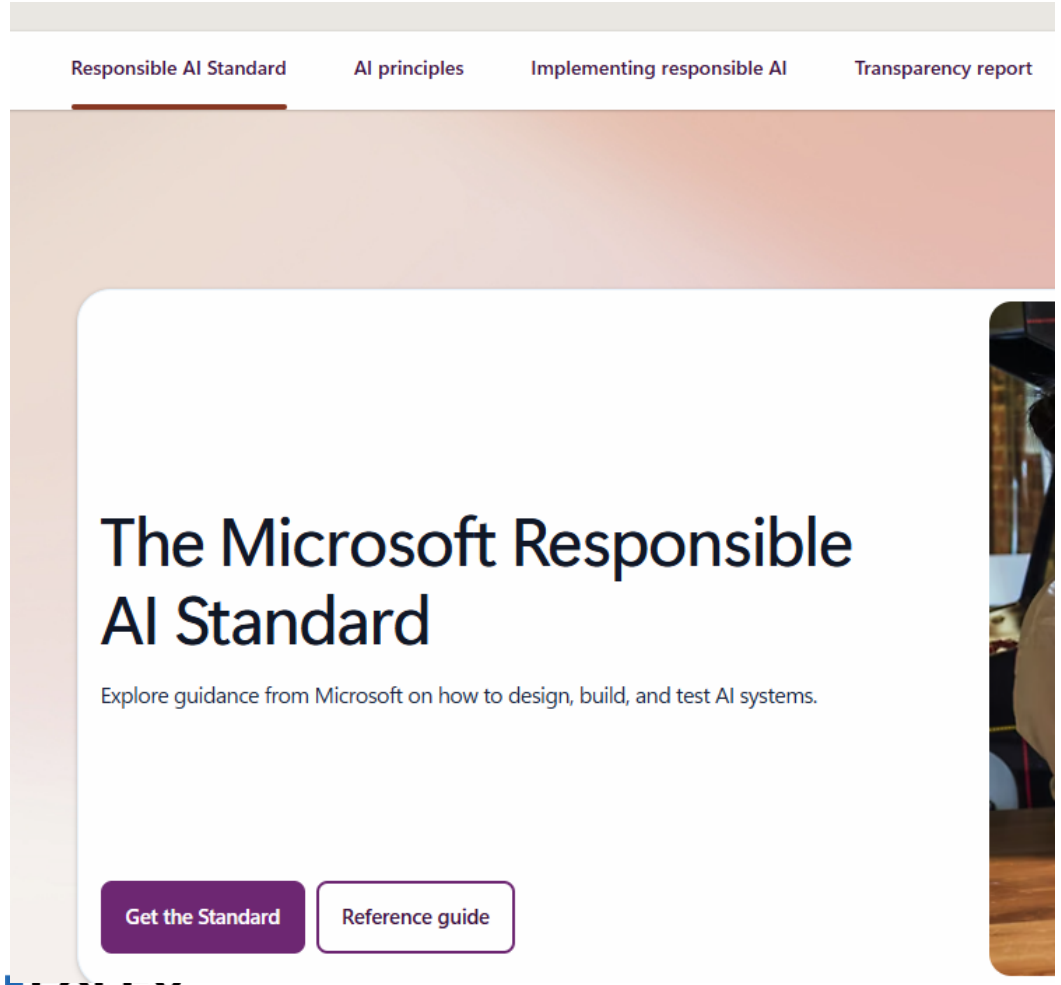
FOLEY

FOLEY & LARDNER LLP

CONFIDENTIAL

Smart AI Governance In 2026

Responsible AI Principles and Approach | Microsoft AI

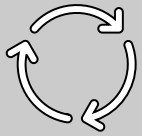


Scan this code to access responsible AI resources from Microsoft

FOLEY & LARDNER LLP

AI Governance Framework

Based on the **NIST AI Risk Management Framework [Govern → Map → Measure → Manage], EU AI Act, ISO/IEC 42001**



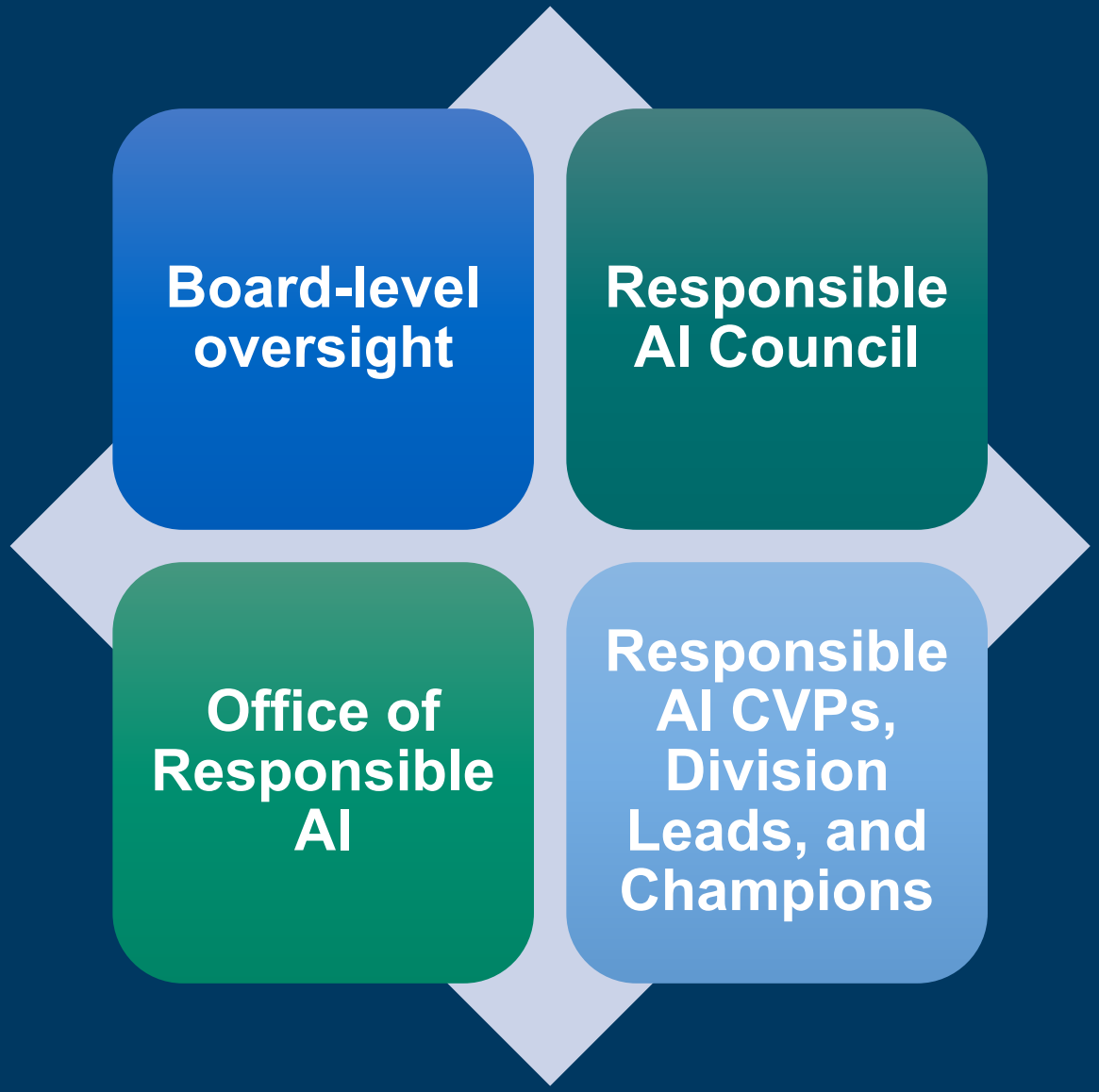
Applied consistently across **model development, product deployment, and post-release operations**

Designed to scale across modalities (text, image, audio, video) and agentic systems

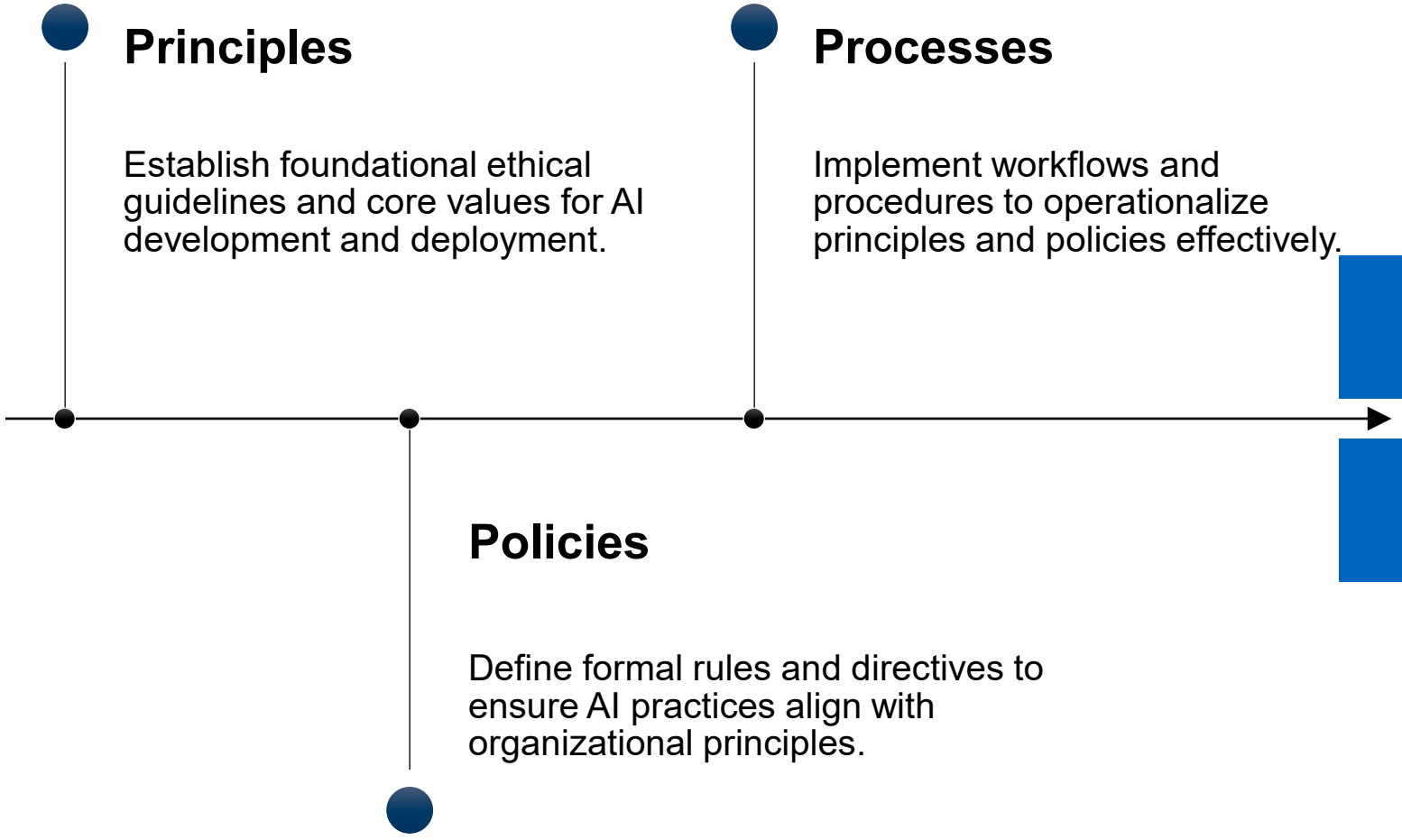
FOLEY

FOLEY & LARDNER LLP

AI Governance structure



Governance: Principles, Policies, Processes



Systematic AI Risk Mapping Ensures Governance

Systematic Risk Mapping

- Required for all AI systems; heightened scrutiny for high-impact use cases
- Methods include:
  - Threat modeling
  - Responsible AI impact assessments
  - Red teaming (centralized and distributed)
  - Customer feedback and incident signals

Adventures in red teaming, 3+ years ago vs today

Prompt: Blonde female ninja on the helm of a sailboat with a bottle of rum, comic book style

FOLEY

FOLEY & LARDNER LLP

High-Risk Use Governance
Sensitive Uses Program

Mandatory Oversight for High-Impact AI

- Applies to systems affecting:
  - Legal status or life opportunities
  - Physical or psychological safety
  - Human rights
- Requires additional safeguards beyond baseline standards

AI Governance Playbook

- **Purpose**: Ensure AI systems are lawful, safe, accountable, and trustworthy across their full lifecycle.
- **Outcome**: Scalable AI innovation with demonstrable compliance, accountability, and public trust.
- **Alignment**: EU AI Act, ISO/IEC 42001, and NIST AI Risk management Framework.

Alignment: EU AI Act, ISO/IEC 42001, and NIST AI Risk Management Framework

Governance Element	EU AI Act	ISO/IEC 42001	NIST AI RMF
Governance Foundation	Risk-based AI governance framework; documented policies for compliance	AI Management System with formal policies and controls	**GOVERN**: Policies, processes, accountability
Executive & Board Oversight	Accountability allocated across AI value-chain roles	Leadership responsibility and oversight	**GOVERN**: Senior ownership
Lifecycle Risk Management	Design → deployment → post-market monitoring	Lifecycle controls and operational processes	**GOVERN / MAP / MEASURE / MANAGE**
High-Risk AI Controls	Enhanced obligations for high-risk & GPAI systems	Risk severity determines control strength	**MAP**: Contextual risk analysis
Risk Identification	Risk analysis & technical documentation	Risk assessment requirements	**MAP**: Identify harms & misuse
Risk Evaluation & Testing	System testing & evidence of mitigation	Performance evaluation & monitoring	**MEASURE**: Test, validate, quantify
Deployment Safeguards	Post-market monitoring & corrective action	Operational controls	**MANAGE**: Mitigate & monitor
Incident Response	Incident reporting & remediation	Incident handling & continual improvement	**MANAGE**: Respond & learn
Supply-Chain Responsibility	Provider vs deployer obligations defined	Third-party & ecosystem controls	**GOVERN**: Ecosystem accountability
Transparency & Documentation	Technical documentation & disclosures	Documented management system	**GOVERN**: Traceability
People & AI Literacy	AI literacy proportional to role & risk	Competence & training requirements	**GOVERN**: Human readiness
Continuous Improvement	Ongoing risk updates	Continual improvement mandate	Framework is iterative by design

Model Cards

MODEL DETAILS

MODEL ARCHITECTURE

TRAINING DATA AND METHODOLOGY

PERFORMANCE METRICS

POTENTIAL BIASES AND LIMITATIONS

RESPONSIBLE AI CONSIDERATIONS

FOLEY

FOLEY & LARDNER LLP

Smart AI Governance Diligence Pressure Points

Challenge

- It becomes difficult to vet AI vendors because limited information is available even through model cards.
- Embedding “black box” generative AI tooling into agentic architecture can present compounded risk.
- New communication protocols are making governance even more difficult.
- Agentic AI architectures present unique challenges around security, accountability, and explainability.

Opportunity

- Demand from your AI vendors: (i) model cards; (ii) bias assessments; (iii) carefully review underlying model security reports.
- Consider implementing additional guardrails over generative systems, such as deterministic systems.
- Ensure security governance frameworks are robust enough to cover agentic AI architectures and developments. Look to CSA for guidance. Ensure security team is aware of the unique security challenges.

Smart AI Governance
Contracting Pressure Points

Data Ownership Challenges

- Definitions of customer data, vendor data, outputs, IP (platforms, models, weights), usage data / telemetry, aggregate, and de-identified data.
- Vendors tend to want to leverage ownership of usage data / telemetry, aggregate, and de-identified data, while enterprises want ownership of customer data.
- Ownership over outputs is a battleground. Most AI software companies are allowing the customer to own the outputs and provide a broad license back to the software provider.
- Future battleground – What does “derivative improvement” include around model retraining?

Potential Solutions

- Enterprise customers are looking at no-training as a default.
- Negotiate permissions to allow for product / service improvements.
- Clearly define derivative improvement rights.
- Watch for conflicting license rights across multiple agreements, DPA, security addendum.
- Develop contracting playbook with must haves, nice to haves, waivable provisions.
- Consider needs 5 years down the road.

Smart AI Governance
Contracting Pressure Points

Risk Allocation Challenges

- Non-deterministic AI will always carry risk and some rate of error. Enterprises are demanding more representations regarding accuracy and reliability. Vendors are pushing back.
- Some enterprise customers are beginning to tie SLA credits to output quality, and third-party validation of quality outputs.
- Some enterprises are beginning to ask for indemnify for downstream harms from the AI system deployment (which can carry into special / incidental / consequential damages).
- Some enterprises are demanding more detailed human-in-the-loop responsibilities by the software vendor.

Considerations

- Consider impact of Workday, where authority will sit. This becomes challenging in the age of agentic AI.
- Consider the impact on consequential harm waivers, business disruption, and data loss.
- Ensure indemnification triggers are clear – do not leave anyone guessing. Map what could “go wrong” early.
- Build contracting playbook.

ISO 42001

- **ISO 42001 is the first certifiable AI management system standard**. Published in 2023, it establishes the requirements for implementing, maintaining, and improving AI management systems.
- **The standard operationalizes responsible AI into auditable controls**. Requires documented processes around AI risk assessments, data governance, transparency, human oversight, bias mitigation, and ongoing monitoring.
- ISO 42001 converts “principles” into structured governance artifacts, internal controls, and audit-ready evidence.
- Potential market differentiator in enterprise procurement.

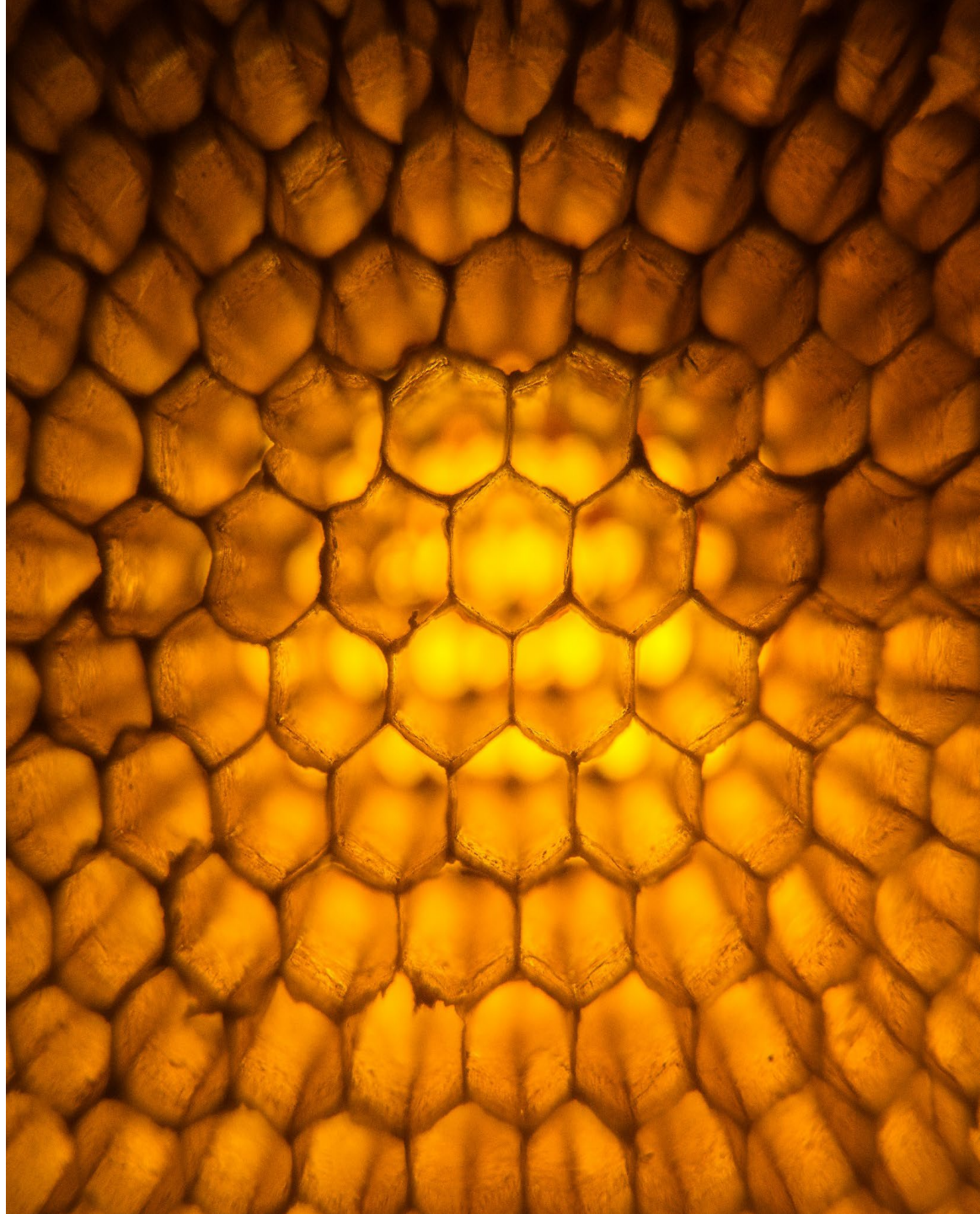
ISO 42001 Roadmap

- **Define AIMS Scope**. Which AI systems are in scope? Consider geographic and business-unit coverage.
- **Obtain Leadership Commitment**. Seek formal approval. Ensure governance policies and documents are authorized. Ensure appropriate management overview is established.
- **Map Context**. Identify key stakeholders, external regulations, and internal objectives.
- **Map Systems**. Complete an inventory of the relevant AI systems, and complete AI risk assessments.
- **Build Controls**. Ensure appropriate controls are in place, including around governance, oversight, data governance, model development and validation, and incident response.

FOLEY
FOLEY & LARDNER LLP

Key Takeaways

- ✓ The global AI regulatory landscape is shifting. **It is possible to take a singular approach**.
- ✓ Create a contract playbook for AI vendors and customers. Know where the battlegrounds lie.
- ✓ Consider ISO 42001 certification around key products to shorten the sales cycle and minimize diligence.
- ✓ Ensure AI governance teams are aligned across internal and external use cases. Be flexible. Scale the program for future uses.



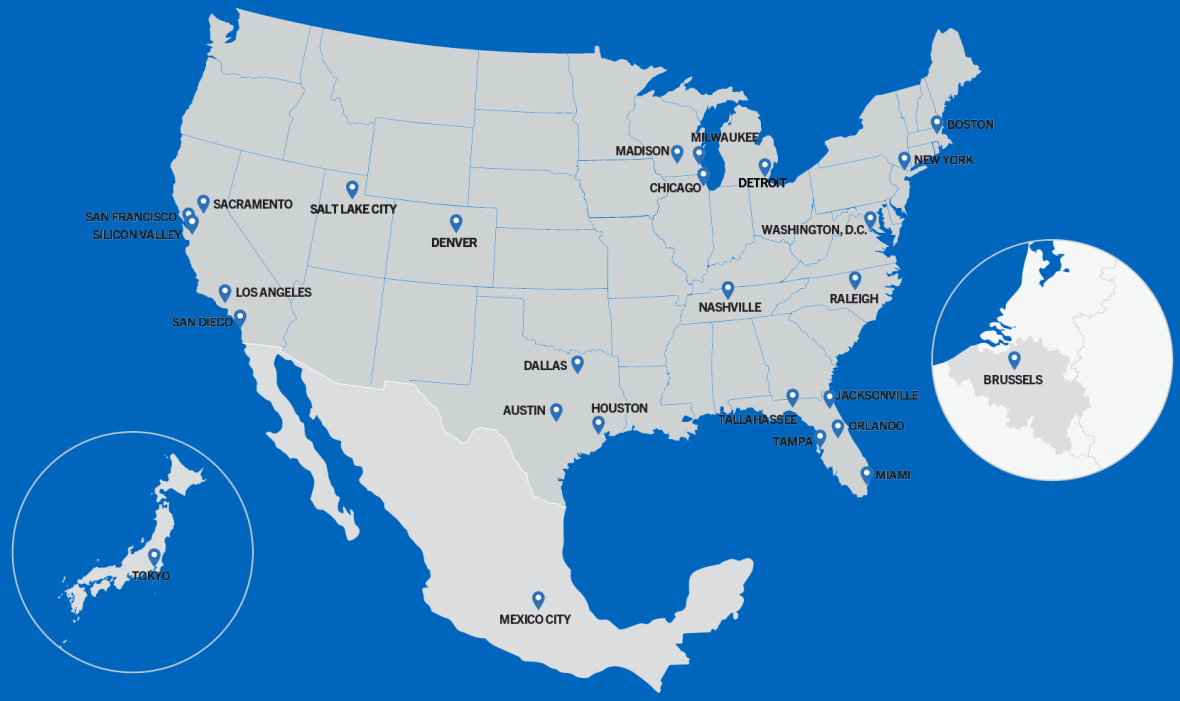
Speaker Bio

- Partner at Foley & Lardner LLP
- Peter helps organizations around the world turn the complex legal and regulatory challenges of AI, data, and emerging technologies into a competitive advantage rather than a roadblock.
- Peter's practice covers the entire lifecycle of technology-driven legal challenges. He drafts and negotiates complex technology agreements. He architects privacy and cybersecurity policies from the ground up. He designs AI governance programs that balance innovation with accountability. He conducts risk assessments and tabletop exercises that prepare organizations for real-world scenarios. And when regulatory inquiries, litigation, or cyber incidents strike, Peter is the steady hand guiding clients through the storm.

About Foley

Foley is an *Am Law* 50 law firm consistently ranked among top-tier practices. We provide an unmatched level of client service, innovation, and value — all tailored to meet your specific needs.

- Providing comprehensive legal services in more than 60 practice areas
- Garnering global recognition for providing exceptional client service and value
- Delivering industry thought leadership at the forefront of business trends and key legal developments and regulations
- Investing in understanding your business, markets, and goals
- Offering alternative fee arrangements and budgets to provide cost efficiencies and certainties



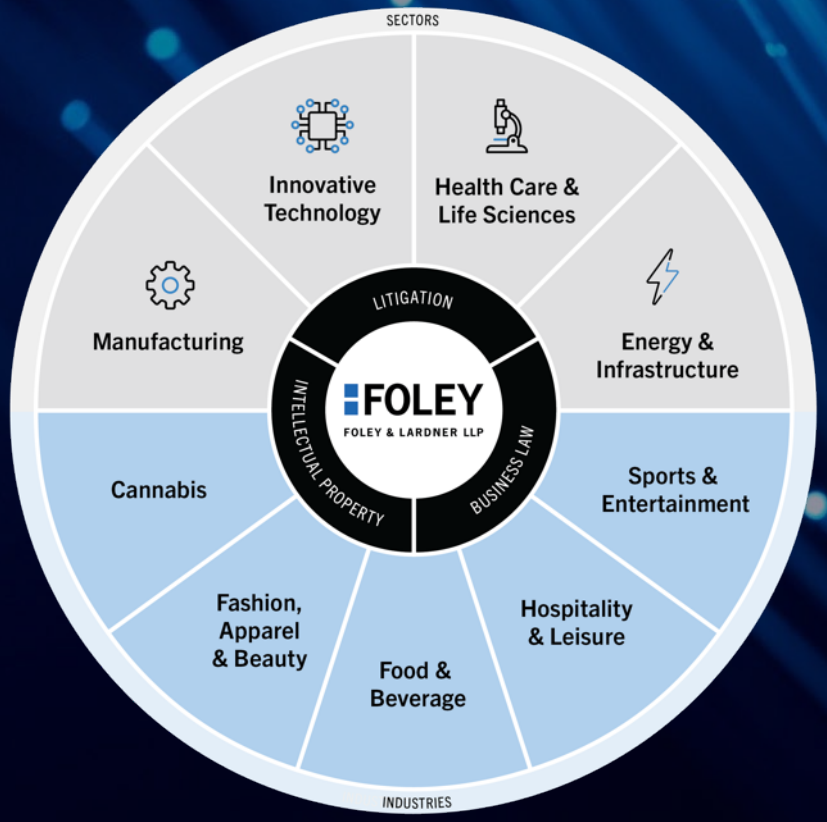
1,100
Attorneys

27
Offices

180+
Years of History

What We Do

We comprehensively and effectively address legal and business matters across four primary sectors and a broad range of industries that align with our clients and strengths.



60+
practices, including:

- Antitrust
- Business Litigation and Dispute Resolution
- Capital Markets and Public Company Advisory
- Commercial Transactions and Business Counseling
- Consumer Law, Finance, and Class Action
- Corporate Governance
- Cybersecurity and Data Privacy
- Environmental
- Employee Benefits and Executive Compensation
- Environmental, Social, and Governance
- Export Controls and National Security
- Government Enforcement Defense and Investigations
- Investment Management and Fund Formation
- IP Litigation
- IP Procurement, Management, and Counseling
- Labor and Employment
- Mergers and Acquisitions
- Private Equity and Venture Capital
- Real Estate
- Securities and Corporate Finance
- Taxation
- Trademark, Copyright, and Advertising Counseling

About Foley

Foley & Lardner LLP is a preeminent law firm that stands at the nexus of the Energy & Infrastructure, Health Care & Life Sciences, Innovative Technology, and Manufacturing Sectors. We look beyond the law to focus on the constantly evolving demands facing our clients and act as trusted business advisors to deliver creative, practical, and effective solutions. Our 1,100 lawyers across 27 offices worldwide partner on the full range of engagements from corporate counsel to intellectual property work and litigation support, providing our clients with a one-team solution to all their needs. For nearly two centuries, Foley has maintained its commitment to the highest level of innovative legal services and to the stewardship of our people, firm, clients, and the communities we serve.

FOLEY.COM

FOLEY

FOLEY & LARDNER LLP

ATTORNEY ADVERTISEMENT. The contents of this document, current at the date of publication, are for reference purposes only and do not constitute legal advice. Where previous cases are included, prior results do not guarantee a similar outcome. Images of people may not be Foley personnel.

© 2026 Foley & Lardner LLP