# Insuring AI

## Navigating the New Coverage Battleground

May 1, 2026

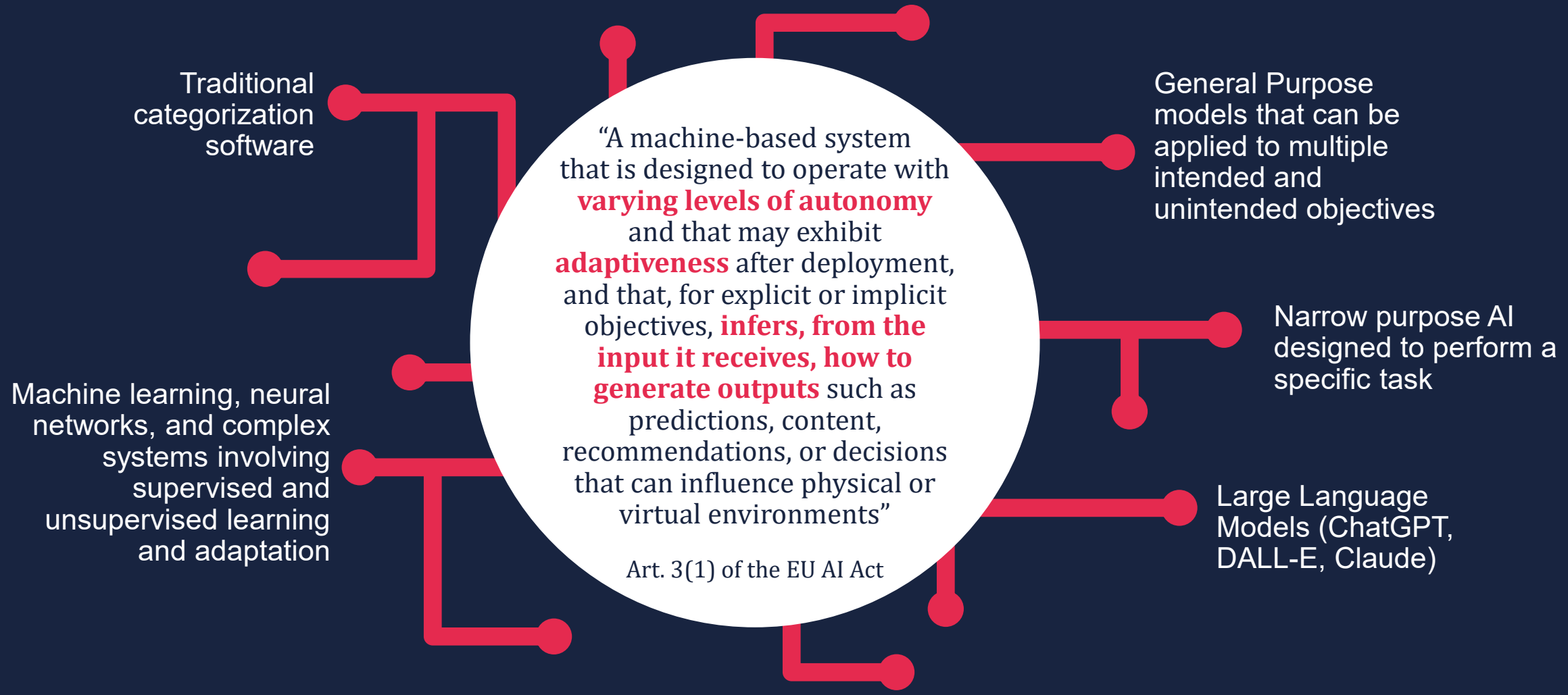
# Presenters

**Kathleen Birrane**
Partner
Business and Commercial
*Baltimore*
Kathleen.Birrane@dlapiper.com

**Neill Thupari**
Partner
Business and Commercial
*Baltimore*
Neill.Thupari@dlapiper.com

**Sean Fulton**
Of Counsel
AI and Data Analytics
*Dallas*
Sean.Fulton@dlapiper.com

# Defining “AI System”



# Legislative Definitions of "AI"

- Legislatures and regulatory bodies across the US and internationally **have not yet reached a consensus** on a single, uniform **definition of "artificial intelligence," but common themes are emerging:**

  - ❑ Emphasis on **machine-based systems** as distinct from human processes.
  - ❑ Characterized by system's **ability to infer or determine outputs** from data rather than following static rules.
  - ❑ Core function is to **produce an output**—e.g. prediction, classification, recommendation, etc.
  - ❑ Adaptive abilities that allow for the **system to change over time**.

**European Union AI Act:** "A **machine-based system** that is designed to operate with **varying levels of autonomy** and that may **exhibit adaptiveness after deployment**, and that, **for explicit or implicit objectives, infers**, from the input it receives, **how to generate outputs** such as predictions, content, recommendations, or decisions that can influence physical or virtual environments"

**Maryland** : Utilization Review HB 820 (2025): "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."

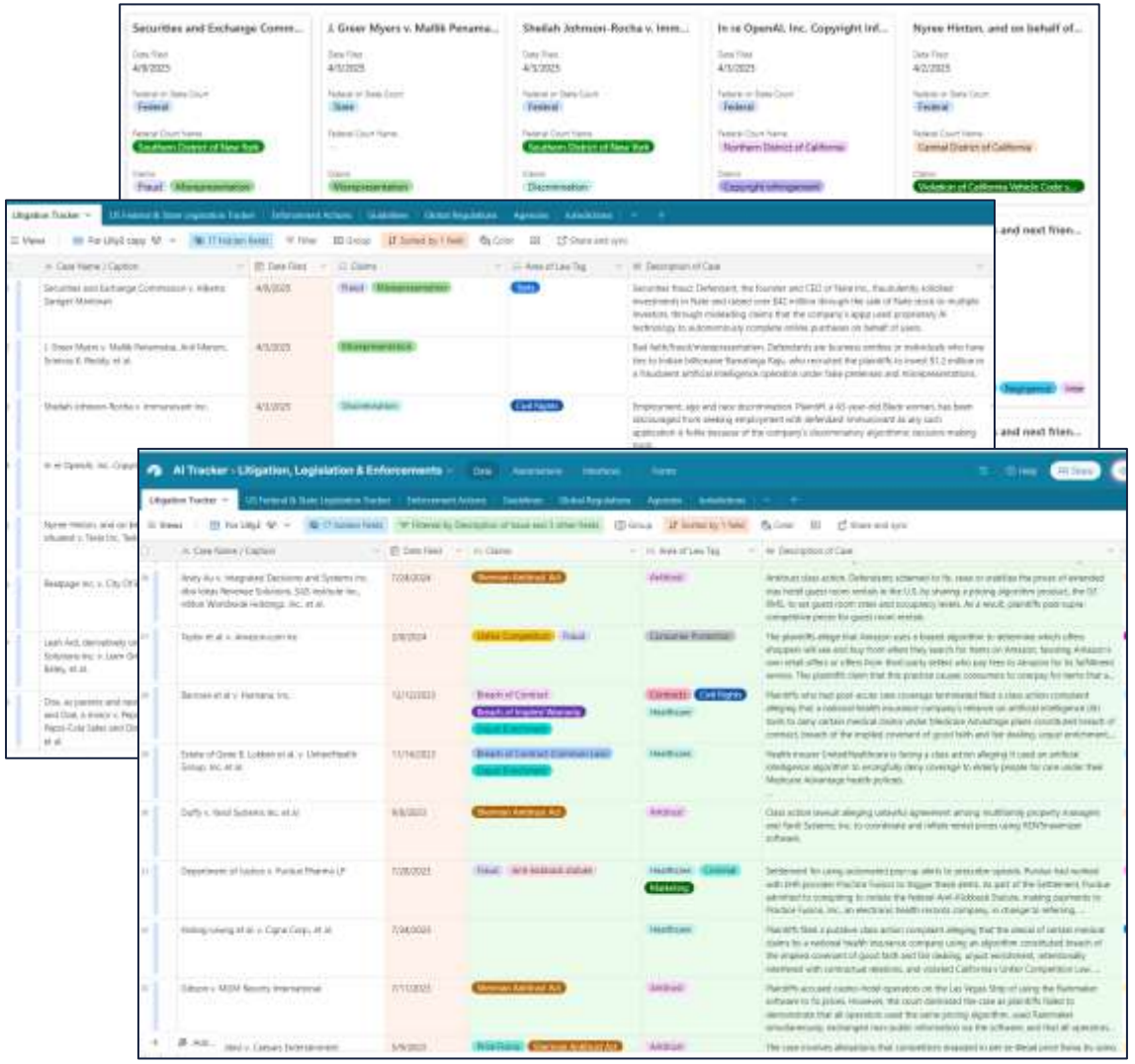
**Colorado SB 24-205 (Concerning Consumer Protections in Interactions with Artificial Intelligence):** "Any **machine- based system** that, for any explicit or implicit objective, **infers from the inputs** the system received how to **generate outputs**, including content, decisions, predictions, or recommendations, that can influence physical or virtual environments"

**New York City Local Law 144 (HR):** "a group of **mathematical, computer-based techniques**: (i) that **generate a prediction** ... or that **generate a classification** ... and (ii) for which **a computer at least in part identifies the inputs**, the relative importance placed on those inputs, and, if applicable, other parameters for the models in order to improve the accuracy of the prediction or classification"

**Utah AI Policy Act:** "an **artificial system** that: (i) is trained on data; (ii) interacts with a person using text, audio, or visual communication; and (iii) **generates non- scripted outputs** similar to outputs created by a human, with **limited or no human oversight**"

# More Than 400 AI Lawsuits

- **Wide Geographic & Subject Matter Net**: Capturing AI-related **litigation**, **claims**, **defenses**, **statutes**, **regulations**, and **theories**
- 180+ cases filed in 2025. Cases include:
  - **IP**: Copyright, trademark, and trade secret cases involving AI training data and outputs
  - **Privacy & Data Protection**: Biometric data, personal information, and consent issues
  - **Securities & Fraud**: AI capabilities misrepresentation and investor issues
  - **Product Liability**: AI system reliability and safety concerns
  - **Constitutional/Civil Rights**: Due process and discrimination claims
- Given growth of AI-related cases, we are exploring ways to **leverage AI to scale this tool with our Innovation team**




*Sample data from DLA Piper's AI Litigation Tracker*

# Key AI Issues

Top-of-mind AI legal and regulatory considerations and trends

**Product Liability:** Claims arising from AI product defects.

**Healthcare AI:** Patient-facing AI, as well as AI that makes medical, coverage, or access determinations, is often "high risk," and additional testing and auditing of such systems may be warranted.

**HR / Internal Use Cases:** Internal enterprise use cases that could impact human safety or rights can form the basis under traditional liability theories (e.g., negligence, employment discrimination).

**Commercial Claims:** Complexities in the AI value chain create unique liability-shifting considerations with commercial partners and customers.

**Customer / Consumer Facing AI:** Using AI to communicate with customers or members of the public raises accuracy and transparency considerations.

**AI Washing:** Company statements about AI risks, capabilities, and limitations are subject to both investor and regulatory scrutiny.

**Complex Regulatory Compliance Requirements:** Multinational companies face hundreds of enacted and proposed AI-specific laws, in addition to existing sector-specific regulations.

**Algorithmic Price Fixing:** Claims that AI-driven pricing tools facilitated unlawful coordination among competitors.

# Product Liability in the AI Era

- Widespread adoption of this technology across sectors and potential to impact large user bases may tip in favor of expanding traditional product liability theories to **remedy harms caused by inaccuracies**.
- Historically, software has been treated as a "service" rather than a "product." However, courts and regulators are showing a willingness to **hold AI developers liable on a strict liability theory** (i.e., without a showing of negligence or fault).
- Theories may translate more easily to **physical AI, but are expanding** to cover digital products and attach strict liability to pure software.
    - ***Garcia v. Character Technologies*** (product claims about Character.AI chatbot allowed to proceed, with recognition of Google's potential upstream liability for supplying technical infrastructure)
    - ***EU Product Liability Act*** expressly includes software/AI, creates a presumption of causation in certain circumstances
- Based on recent examples in Canada, courts may be willing to **hold companies liable for misstatements generated by AI** under more traditional theories of liability.

# Chatbots Pose Unique Litigation and Enforcement Risks





- Demonstrating how hard it is to regulate AI, the EU AI Act categorizes many chatbots as "limited risk" AI – yet chatbots are driving AI liability and reputational harm.
- Lawsuits have been filed against seeking to hold companies responsible for their chatbots' alleged harms or misstatements, including on pricing and company policy.
- State AGs and the FTC are launching investigations and requiring companies to turn over internal analyses on the impact of their technologies on vulnerable users.
- The political and legal climate is ripe for MDL, class action, or other mass plaintiff claims to sweep in all major AI providers and deployers.

# Increasing Focus on Accuracy of AI Claims

Investors, consumers, and regulators are holding companies accountable for making allegedly false or deceptive claims about AI.

- In January 2026, the FTC announced a settlement with Growth Cave, resolving allegations that the **company misrepresented that its "AI software" would "automate nearly 100% of the process"** of setting up and operating an online education course.
- Part of a growing trend over the past year:
  - **At least 17 securities AI-related class actions were filed in 2025,** compared to 14 in 2024 and 7 in 2023, alleging that investors were misled about companies' AI strategies or products.
  - **4 FTC cases were filed in 2025 (12 since 2024)** targeting deceptive claims about AI and automated tools, including in the B2B context and across a wide variety of products.
  - In September 2024, the Texas Attorney General agreed to a **settlement with an AI healthcare company**, resolving allegations about **deceptive accuracy and safety claims**, and imposing marketing restrictions and disclosure obligations.

"If a company is raising money from the public, though, it needs to **be truthful about its use of AI and associated risk**."

AI companies offering products used "in high-risk settings owe it to the public and to their clients to be **transparent about their risks, limitations, and appropriate use**."

- Texas AG Ken Paxton

# HR AI Tools Have Immense Promise, but Raise Unique Risks

Private litigants and lawmakers are focused on employment AI

- HR AI tools are among the most common **"high risk" internal use** cases for large organizations.
  - Subject to mandatory bias testing and notice/disclosure requirements under US state AI laws and the EU AI Act
- We have already seen **employment discrimination claims** arising from use of AI tools in the hiring process.
- **Internal controls** are key to managing residual risks.
  - Best practices include: human decisionmaking, responsible use of candidate/employee data, training for HR/talent acquisition, clear disclosures, and documented bias mitigation efforts

Common use cases and tools available on the market include:

- **Resume scanners** that prioritize or score applications that meet certain criteria
- **Virtual assistants or chatbots** that ask candidates about their qualifications, answer questions about the organization or specific job openings, or suggest open positions
- **Video interview software** that transcribes, generates insights, and/or evaluates candidate performance
- **Testing or training software** that measures candidates or employee performance or skills
- **Employee monitoring software** that rates and tracks employees based on their performance or activities
- **Performance evaluation** processes, including drafting and data analytics for use in self-evaluations
- **Compensation analytics**, including market benchmarking, pay equity analysis, and forecasting

# AI Raises Unique Contracting Considerations

- For any AI solution, there may be a number of **key stakeholder groups** involved.
- Each of these stakeholder groups have **distinct responsibilities and exposure to risk**.
- Risks associated with AI solutions are **not always clearly assigned**.
- Risk-based procurement frameworks to distinguish and address **low-impact vs. high-impact** AI use cases are becoming a best practice.
- Vendor **due diligence and risk assessment** processes should address AI-specific issues (e.g., data rights, ownership/control over inputs and outputs, testing and monitoring).

**AI-Specific Provisions are critical to address:**

- Lack of clarity and transparency in the AI supply chain
- Compliance with AI laws
- Access to AI testing, validation, and other system information
- Intellectual property loss
- Privacy and security concerns
- Indemnity for AI claims and litigation risk exposure

# DOJ, FTC, and State AGs have pursued algorithmic price fixing. We can test and vet your models.

**April 6, 2015**

Former E-Commerce Executive Charged with Price Fixing in the Antitrust Division's First Online Marketplace Prosecution

**August 23, 2024**

Justice Department Sues RealPage for Algorithmic Pricing Scheme that Harms Millions of American Renters

- DOJ, FTC, and State Attorneys General have publicly addressed concerns about the use of algorithms for price fixing.
- Both DOJ and FTC make clear that using algorithms to fix prices is illegal. The past decade has seen the first prosecutions as well as civil suits brought on allegations of using algorithms to price fix.
- In the franchise context, ***centralized pricing and even price setting led by the franchisees may present unique challenges if AI is used, even in part, to set these prices***.
- We regularly test and evaluate AI models that compare competitive pricing across an industry and work with clients to develop mitigation strategies that minimize associated enforcement risks.
- This testing enables us to surface risks early, including gaps in data siloing and protection against non-public information being shared with competitors, helping clients to proactively manage enforcement and litigation risk.

# Impact of AI Litigation on Insurance: What Policies May Be Triggered

- **Technology E&O/Professional Liability:** Inaccurate AI advice, hallucinated output, defective software, failed automation
- **Cyber/Privacy:** Data leaks, privacy law violations, biometric claims, model inversion, prompt-injection breach
- **D&O:** Governance failures, lack of oversight, regulatory investigations, securities litigation, and AI washing
- **CGL:** Bodily injury, property damage, advertising injury, or defamation deriving from or caused by AI
- **Media/IP Liability:** Output infringement, false light, copyright training-data suits
- **Crime/Social Engineering:** AI-enabled impersonation, fake invoice schemes, deepfake voice fraud
- **EPLI:** AI hiring tool bias, promotion/termination algorithm discrimination

# “Silent AI” Exposure and the Possible Ramifications

- Policies not written for or in contemplation of AI may be at risk.
- Insureds and insurers alike must consider AI-specific provisions (i.e., exclusions and endorsements).

# Policy-Response Trends

- AI-Specific Exclusions and Endorsements
- Changes in Underwriting Approaches
- Standalone AI Insurance/Specialty Coverage Offerings
- AI-Based Litigation (including Bad Faith)

# What We've Seen Thus Far: AI-Based Litigation Involving Insurance

- AI Denial of Health Benefits
- Algorithmic Discrimination in Claims Handling
- Telematics/Driver Data Analytics
- Algorithmic Pricing/Antitrust
- Legacy Claims-Valuation Software/Bad Faith Algorithm

# AI-Based Litigation on the Horizon

- More Algorithmic Lawsuits (Bad Faith, Discrimination, Antitrust)
- Privacy, Data, and Biometric Actions
- **Coverage Litigation?**
  - *United States Liability Ins. Co. v. Retsel Corp.* (D. Neb.)

# Key Takeaways

## Check Your Policies Carefully and Mitigate Potential Liability Claims

- Looking Ahead, Examine Underwriting Practices and Consideration of Exclusions/Endorsements to Limit Exposure

## The Majority of Anticipated Litigation Is Trending Towards Two Categories

- **Algorithmic** (Discrimination, Bad Faith, Antitrust)
- **Privacy/Data/Biometric** (Statutory, Regulatory, and Consumer Protection)

## Mature Body of AI-Insurance Coverage Case Law Does Not Exist, But Challenges May Be Coming

# Thank you



DLA PIPER