IADC COMMITTEE NEWSLETTER

Product Liability

October 2026

In This Issue

What a wonderful Roundtable at Pfizer headquarters in New York City! Many of you joined us for informative and fun presentations at this year's Product Liability Roundtable. It was great to see so many of you! We appreciate the contributions of everyone who developed this program and encourage anyone interested in getting involved next year. If you were unable to attend the Roundtable, here's a part of what you missed. With the EU's AI Act and new Product Liability Directive demanding accountability for AI, together with the proposed US AI LEAD Act, 2026 marks a pivotal year for AI as the legal framework governing its risks continues shifting from voluntary guidelines to hard liability. This article analyzes the updated EU Product Liability Directive which formally classifies AI as a "product," alongside the proposed US AI LEAD Act which seeks to do the same. It then examines the collision of technological innovation with legal responsibility, focusing on how manufacturers can prepare for a more litigious, heavily regulated AI landscape.

The "Black Box" of AI: No Longer A Legal Shield for Product Manufacturers

About the Authors



Phil Goldberg is the office managing partner of Shook, Hardy & Bacon LLP in Washington, D.C., and co-chair of the firm's Public Policy Practice Group. He has more than 25 years of experience advising clients on high stakes and high profile liability-related public policy, public affairs, and public relations issues. He can be reached at pgoldberg@shb.com.



Katie Maechler is a partner at Maslon LLP in Minneapolis, where she co-chairs the firm's Litigation and Tort & Product Liability groups and is ranked Band 1 in Product Liability Litigation in Minnesota by Chambers USA. With 20 years of experience, she represents national and multinational manufacturers in complex product liability matters and advises clients on CPSC compliance, recalls, and reporting. She can be reached at katie.maechler@maslon.com.



Greg Williams is a partner at Clayton Utz and a product liability practitioner with more than 25 years of experience defending complex claims and class actions involving pharmaceuticals, medical devices, financial services, and automobiles. He also advises pharmaceutical and medical device companies on regulatory matters throughout the product lifecycle, has particular expertise in pricing and reimbursement, and holds a master's degree in biochemistry. He can be reached at gwilliams@claytonutz.com.

*The **International Association of Defense Counsel** serves a distinguished, invitation-only membership of corporate and insurance defense lawyers. The IADC dedicates itself to enhancing the development of skills, professionalism and camaraderie in the practice of law in order to serve and benefit the civil justice system, the legal profession, society and our members.*

***w: www.iadclaw.org p: 312.368.1494 e:** dleon@iadclaw.org*

About the Authors Continued



Lisa DeBord is Senior Assistant General Counsel on Bayer's Global Litigation team, where she manages complex litigation across the United States. In that role, she also has a particular interest in the evolving use of artificial intelligence and emerging legal technologies to support litigation strategy, efficiency, and risk management. She can be reached at lisa.debord@bayer.com.



Dr. Michael Malterer is an M&A and Automotive Regulatory partner at Dentons, where he leads the firm's Automotive sector teams in Germany, Europe, and globally and co-leads its Global Autonomous Vehicles team. With 25 years of experience, he advises automotive manufacturers, suppliers, technology companies, and private equity funds on M&A and regulatory matters involving connectivity, autonomous driving, new mobility, and electrification. He can be reached at michael.malterer@dentons.com.



Danielle Mindlin is the Assistant General Counsel at Pfizer Inc. Danielle has been with Pfizer for over nine years. Danielle earned her JD from the NYU School of Law. She can be reached at Danielle.Mindlin@pfizer.com.

About the Committee

The Product Liability Committee serves all members who defend manufacturers, product sellers and product designers. Committee members publish newsletters and *Journal* articles and present educational seminars for the IADC membership at large and mini-seminars for the committee membership. Opportunities for networking and business referral are plentiful. With one listserv message post, members can obtain information on experts from the entire Committee membership. Learn more about the Committee at www.iadclaw.org. To contribute a newsletter article, contact:



Marie Chafe
Vice Chair of Newsletters
Conn Kavanaugh Rosenthal Peisch & Ford, LLP
MChafe@connkavanaugh.com

I. Introduction

Artificial intelligence is no longer a futuristic abstraction. It is embedded in the products we use, the decisions companies make, and the systems that govern access to employment, credit, healthcare, and transportation. As AI proliferates across the product life cycle—from design and manufacturing to post-sale monitoring and consumer-facing recommendations—so too does the potential for harm and the potential for liability. Legislative bodies, courts and others on both sides of the Atlantic have taken notice and are beginning to establish rules for who is liable to whom and under which liability theories for AI-caused harm.

2026 marks a pivotal year. The European Union has adopted a comprehensive regulatory scheme that expressly classifies AI as a "product" subject to strict liability, while simultaneously imposing technical compliance obligations, a breach of which triggers presumptions of defect. In the United States, the landscape remains fragmented. A patchwork of state-level initiatives, common-law theories, and now a proposed federal statute that would, for the first time, also bring AI systems within the ambit of products liability law. Meanwhile, the American Law Institute has undertaken an ambitious project to articulate principles governing civil liability for AI—an effort that, while still in preliminary form, signals how courts may approach these claims in the near term.

The common thread across these developments is unmistakable: AI's opacity—the so-called "black box"—is no longer a shield for developers and deployers of this technology. It is increasingly a trigger for adverse presumptions, heightened disclosure obligations, and expanded liability. This paper surveys the current legal landscape and offers practical guidance for product manufacturers and others in navigating this rapidly evolving terrain.

II. The European Framework: AI as a Product

The EU has taken a deliberate, centralized approach to AI regulation—one that pairs a revised strict-liability regime with a technical compliance rulebook. Together, the Product Liability Directive and the AI Act create an integrated framework in which regulatory non-compliance feeds directly into civil liability.

A. The Product Liability Directive

Directive (EU) 2024/2853 represents the most significant reform to EU product liability law.[1] Its central innovation for present purposes is definitional: "product" now covers software, including AI systems, alongside electricity, digital manufacturing files, and raw materials. Open-source software developed outside a commercial context is excluded, but any AI system placed on the market in the course of business falls squarely within scope.

The Directive imposes strict liability on manufacturers for harm caused by defective products. A product is defective if it fails to provide the safety that a person is entitled to expect, violates an obvious safety rule, or exhibits an obvious malfunction in normal use. Critically, the Directive now covers post-sale conduct: a bad update, or a security patch that arrives too late, can

[1] Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC.

give rise to liability even if the product was safe at launch.

The Directive's most consequential provisions concern the burden of proof. Causation is presumed once a claimant demonstrates a defect and the harm is of the type that defect would typically produce.[2] Where the technical complexity of the product makes proof excessively difficult for the claimant—as is often the case with AI—courts *must* presume both defect and causation.[3] If the manufacturer refuses to disclose evidence, the court presumes a defect. The black box, in short, now works against the manufacturer.

The liability chain ensures claimants always have a viable defendant within the EU: the manufacturer is primary, but if unavailable, claimants may pursue the importer, authorized representative, distributor, or any party who substantially modified the product.[4] Where a manufacturer incorporates a third-party AI model, the manufacturer remains the primary defendant. There is no cap on damages, and recoverable harm now includes psychological injury and data loss.[5] The statute of limitations runs three years from knowledge, ten years from sale, and twenty-five years for latent personal injuries. Member states wishing to adopt the Directive must transpose the Directive into national law by December 9, 2026.[6]

B. The AI Act

Regulation (EU) 2024/1689—the AI Act—is the EU's technical rulebook for artificial intelligence.[7] It applies directly across all member states without requiring national transposition. Everything in the Act turns on a threshold definition. Article 3(1) defines an "AI system" as 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.[8] The operative element is inference. Software that merely executes rules a human has written, performs basic data processing, or applies classical heuristics does not infer and falls outside the Act altogether. The Act classifies AI systems by risk: prohibited (banned outright), high-risk (subject to strict compliance obligations), limited-risk (transparency duties), and minimal-risk (voluntary codes only).[9] High-risk systems—including those used in critical infrastructure, employment, creditworthiness, and law enforcement—face the most demanding requirements: robust data governance, technical

[2] Directive (EU) 2024/2853, art. 10.

[3] *Id*., art. 10(4).

[4] *Id*., art. 8.

[5] *Id*., art. 6.

[6] *Id*., art. 18.

[7] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence (AI Act).

[8] *Id*., art. 3(1); see also Recital 12. The Commission has issued non-binding guidelines on the boundary. See European Commission, Guidelines on the Definition of an Artificial Intelligence System Established by the AI Act (Feb. 6, 2025). The line between AI systems and conventional software remains contested, and adaptiveness is permissive ("may"), not required.

[9] *See generally Id*.

documentation, human oversight, accuracy and security standards, and ongoing post-market monitoring.

C. How the Regimes Interact

The AI Act and the Product Liability Directive are designed to operate in tandem. A breach of the AI Act's requirements—for data quality, transparency, logging, or risk management—can establish a presumption of defect under the Product Liability Directive. The AI Act's compliance checklist thus becomes the plaintiff's checklist. The two instruments do not, however, share a scope. The Product Liability Directive attaches to software as such under Article 4(1) and never adopts the Article 3(1) definition; it reaches AI only because AI systems are software, with the recitals confirming that providers of AI systems within the meaning of the AI Act are to be treated as manufacturers.[10] A system that falls short of Article 3(1) therefore escapes the AI Act but remains a product subject to strict liability.

Liability crystallizes at three points in the product life cycle. At *design*, a manufacturer that skips proper training, testing, or decision-logging exposes itself to both AI Act sanctions and product liability claims. At *training*, biased or incomplete data supports a presumption of defect—and because AI systems evolve post-sale, a bad update creates fresh liability. At *warnings*, poor documentation of an AI system's limitations constitutes both an AI Act violation and a failure-to-warn claim under the Product Liability Directive.

For manufacturers, the practical implications are clear. Documentation must be comprehensive and maintained in plain language: design choices, training-data provenance, risk assessments, and post-launch monitoring protocols. Contracts along the AI supply chain require fresh scrutiny—indemnities, warranty limitations, and insurance obligations must account for the Directive's expanded scope. And standard product liability insurance may not adequately cover the ongoing, life cycle-based exposures that AI products create.

III. The United States: A Fragmented Landscape

Unlike the EU's comprehensive framework, the United States has no unified federal regime governing AI liability. The result is a patchwork of state laws, regulatory guidance, and common-law theories that create significant compliance challenges—particularly for companies with interstate or multinational operations.

Historically, plaintiffs pursuing AI-related harms have relied on adjacent legal theories: consumer protection, privacy, defamation, negligence, and intellectual property. Courts have generally treated AI outputs as expressive or informational content rather than tangible products subject to strict liability or design-defect analysis. Defendants have leveraged this characterization, invoking First Amendment protections and Section 230 immunity to argue that AI-generated outputs are protected speech, not actionable product defects. This doctrinal posture has frustrated plaintiffs seeking to apply traditional products-liability frameworks to AI systems.

Against this backdrop, two parallel developments are reshaping the U.S. landscape: proposed federal legislation that would, for the first time, classify AI systems as "products" for liability purposes, and an American Law Institute project articulating

[10] Directive (EU) 2024/2853, art. 4(1); Recital 13.

principles for civil liability that courts may adopt as persuasive authority.

A. The AI LEAD Act

On September 29, 2025, Senators Dick Durbin (D-IL) and Josh Hawley (R-MO) introduced the AI LEAD Act.[11] The bill responds directly to the threshold question that has stymied AI product liability litigation in the United States: whether AI systems constitute "products" subject to traditional liability frameworks. The Act answers in the affirmative, defining AI systems as "covered product[s]" under federal law.[12]

Breadth of Definition. The Act defines artificial intelligence expansively: "*any software*, data system, application, tool, or utility . . . capable of *making or facilitating* predictions, recommendations, actions, or decisions for a given set of human- or machine-defined objectives . . . that uses machine learning algorithms, statistical or symbolic models, or other algorithmic or computational methods (*whether dynamic or static*) that affect or facilitate actions or decision-making in real or virtual environments."[13] The phrase "or facilitating" extends coverage beyond autonomous AI to decision-support tools, analytics platforms, and recommendation engines. The inclusion of "statistical or symbolic models" could capture conventional software predating the generative AI era. This definition is broader than the AI Act's in two respects. The AI Act requires that the system infer its outputs; the LEAD Act expressly reaches static computational methods, and thus rule-based legacy software that Brussels leaves untouched. And the AI Act regulates the system itself, while "or facilitating" extends the LEAD Act to tools that merely inform a human decision.

Expanded Harm. The Act departs significantly from traditional products liability by encompassing financial and reputational injury, behavioral manipulation "highly offensive to a reasonable person," and derivative losses.[14] The AI LEAD Act would allow recovery for harms that may be difficult to quantify or trace to a specific AI output.

Four Causes of Action Against Developers. The Act establishes: (1) negligent design, which requires proof of a reasonable alternative design unless the product is "manifestly unreasonable"; (2) negligent failure to warn; (3) breach of express warranty; and (4) strict liability for a defective condition that is unreasonably dangerous.[15]

Defense Limitations. Regulatory compliance does not preclude a finding of defect as a matter of law, though non-compliance may establish defect.[16] The open-and-obvious defense is limited for users under eighteen.[17] No privity of contract is required for strict liability claims.[18]

Deployer Liability. The Act imposes liability on deployers who substantially modify or intentionally misuse AI systems.[19] "Substantial modification" requires a deliberate, unauthorized change that

[11] S. 2937, 119th Cong. (2025) (AI LEAD Act, introduced Sept. 29, 2025 by Senators Durbin (D-IL) and Hawley (R-MO)).

[12] *Id.*, § 3(3).

[13] *Id.*, § 3(1)(emphasis added).

[14] *Id.*, § 3(8).

[15] *Id.*, § 101(a).

[16] *Id.*, § 101(b)(4)(A)–(B).

[17] *Id.*, § 101(c)(4)(B).

[18] *Id.*, § 101(d)(1)(B).

[19] *Id.*, § 102(a).

alters the product's purpose or function.[20] Joint and several liability applies where both developer and deployer contributed to the harm.[21]

Contractual Prohibitions. The Act prohibits "unconscionable" contractual terms that waive rights, proscribe forums, or unreasonably limit liability.[22] This directly challenges standard AI vendor practices—liability caps, forum-selection clauses, and mandatory arbitration provisions. The Act also establishes a four-year discovery-based limitations period[23] and grants enforcement authority to federal and state attorneys general.[24]

Outlook. As of August 2026, the bill remains in the Senate Judiciary Committee with no hearing held and no House companion bill. Its prospects are uncertain, particularly given Senator Durbin's planned retirement and the current administration's stated preference for a "minimally burdensome" framework.[25] Nonetheless, the Act should not be dismissed. It represents a bipartisan template for where federal liability standards may converge—and plaintiffs' counsel will invoke its framework in current litigation under existing state law.

B. The ALI Principles Project

In 2024, the American Law Institute, which produces a wide range of legal treatises including the Restatements of the Law, convened a project titled "Principles of the Law: Civil Liability for Artificial Intelligence."[26] This is a principles project, not a Restatement, and is intended to assist judges in applying existing common-law doctrines to AI harm, to recommend how the common law could evolve, and to guide legislators. Though still in preliminary form, this project merits attention because ALI projects carry persuasive authority in American courts.

So far, there have been two preliminary drafts issued covering only a portion of the principles the project will ultimately entail. Preliminary Draft No. 2, which was issued in May 2026 and replaces the first draft, employs both negligence and strict liability principles. Here is where things stand:

Framework: The current draft endorses negligence as the baseline for anyone who distributes, provides, or releases an AI model or system, with strict products liability applying to AI models and systems with product-like functionalities. For example, if the AI system wrongly concludes that "there is no obstruction in the roadway," and that misinformation causes injury, the resulting litigation could be brought under products liability. But, if the AI system merely provided advice as to the path a user should take, it would be subject to negligence instead.

Negligence: Under the negligence framework, anyone who distributes, provides, or releases an AI model or system is considered a "Distributor" and

[20] *Id.*, § 3(11).
[21] *Id.*, § 302(c).
[22] *Id.*, § 201(b)(1).
[23] *Id.*, § 303(a)–(b).
[24] *Id.*, § 301.
[25] Exec. Order No. 14365, 90 Fed. Reg. 101,243 (Dec. 11, 2025) (calling for "minimally burdensome national policy framework for AI").
[26] American Law Institute, *Principles of the Law: Civil Liability for Artificial Intelligence*, Preliminary Draft No. 2 (May 2026) (discussed June 2026). The project is led by Reporter Mark Geistfeld (NYU Law) and Associate Reporter Ketan Ramakrishnan (Yale Law).

owes a duty of reasonable care for the model's safety performance and inferential capabilities. Because AI models can be updated, a materially altered model or system triggers a new "release" with its own foreseeability and state-of-the-art baseline. Providers with ongoing access owe a duty that evolves with newly learned risks.

The AI Stack. What reasonable care requires is calibrated to the actor's position in the "AI Stack"—the layered chain running from foundation-model developers through fine-tuners, deployers, and platform operators. Foundation-model developers bear primary obligations for training-data curation, architecture, guardrails, and safety testing. Fine-tuners and deployers inherit calibrated obligations based on their narrower access and control but cannot escape liability by pointing upstream. Platform operators may be treated as Distributors if their operational control and commercial stake are analogous to conventional distributors. Multiple Stack participants can be concurrent tortfeasors, with liability apportioned under comparative-fault principles.

Commercial Distributors. Entities in the business of distributing AI models or systems face enhanced duties requiring them to demonstrate "expert-level" care, testing, and state-of-the-art awareness. Industry custom is evidence, not conclusive proof, of reasonable care. The expert care standard has generated debate, with critics saying it is unworkable for downstream sellers (e.g., a hardware store selling an AI-powered lawnmower). The Reporters agreed to take a new look at this part.

Strict Liability for Product-Like Functionality. The draft identifies four categories triggering strict liability for Commercial Distributors: (1) outputs governing the safety of a cyber-physical system, as with an autonomous vehicle; (2) outputs representing facts that determine access, deployment, or use; (3) outputs classifying existing physical states; and (4) performance benchmarked against human behavior for safety purposes. The dividing line between negligence and strict liability—whether the AI system merely provides guidance versus reaching a safety-critical conclusion—has also drawn significant criticism. It could subject distributors to different liability regimes based on the content of a given output and fortuity of a user's prompt or other inputs.

The principles project remains in its early stages. No draft has been approved by the ALI, and additional chapters, including those addressing deployer and user-as-operator liability, have not yet been drafted. The next advisory committee meeting is scheduled for October 30, 2026. Defense counsel should monitor these developments closely: even in draft form, the principles articulate the analytical framework courts may apply.

IV. Practical Implications for Product Manufacturers

Across these three frameworks—EU legislation, the proposed AI LEAD Act, and the ALI Principles—a consistent set of practical imperatives emerges for product manufacturers and their counsel.

Documentation. Every framework rewards comprehensive, contemporaneous documentation and penalizes its absence. Under the EU Product Liability Directive, failure to disclose triggers a presumption of defect. Under the AI Act, the absence of required logs and risk assessments constitutes a regulatory violation. Under the ALI Principles, documentation bears directly on whether a Distributor exercised reasonable care. And under the AI LEAD Act, the inference-of-defect provision means that manufacturers without

evidence to rebut the inference will face liability by default. Companies should maintain—in plain language, accessible to non-experts—records of design choices, training-data provenance, validation protocols, post-deployment monitoring, and known limitations.

AI Supply-Chain Contracts. Standard vendor agreements are inadequate for the emerging liability environment. Both the EU Directive and the AI LEAD Act impose liability on parties who incorporate third-party AI models—and the AI LEAD Act's prohibition on "unconscionable" terms directly challenges liability caps, forum-selection clauses, and mandatory arbitration provisions. Companies must reassess indemnification provisions, warranty limitations, data-access rights, and insurance obligations throughout the AI supply chain. Under the ALI framework, "substantial participation" in another's safety decisions creates commensurate obligations regardless of contractual allocation.

Insurance. Standard product liability coverage may be insufficient for AI-related exposures. AI products create life cycle-based risks—evolving post-sale through updates, retraining, and ongoing data ingestion—that do not fit traditional occurrence-based policies. The EU's removal of damages caps and expansion of recoverable harm (including psychological injury and data loss), combined with the AI LEAD Act's broad harm definition (including financial and reputational injury), means that potential exposure is significantly greater than under legacy product liability regimes. Companies should engage insurers and brokers to evaluate whether existing programs adequately address these risks.

Monitoring Legislative Developments. The regulatory landscape is moving fast. The EU's December 2026 transposition deadline is imminent. The AI LEAD Act, while not current law, represents a bipartisan template whose framework will inform litigation strategy regardless of enactment. The ALI Principles, though preliminary, will shape judicial reasoning. Defense counsel must track these developments and prepare clients for a liability environment that penalizes passivity and rewards proactive compliance.

The black box of AI is no longer a legal shield—it is a trigger for presumptions, disclosure obligations, and expanded liability. Companies that document rigorously, contract carefully, and prepare proactively will be positioned to defend claims. Those that do not will find the law's assumptions running against them.

Past Committee Newsletters

Visit the Committee's newsletter archive online at www.iadclaw.org to read other articles published by the Committee. Prior articles include:

MARCH 2026
The Fall of Chevron: How the End of 40 Years of Precedent May Impact the Product Liability Practice
Jennifer A. Creedon and Katherine R. Kossoy

JANUARY 2026
Are Digital Applications Products? May the Best Analogy Win
Jason Rose, Sarah Scott, and Christian Coward

NOVEMBER 2025
Food for Thought: A New Frontier of Product Liability Litigation for Ultra-Processed Foods
Elizabeth Sorenson Brotton, Shelley K. Napolitano, and Kyle R. Heim

FEBRUARY 2025
The Dust Settles on Causation: Tippin Decision is a Big Win for Talc Defendants
Elizabeth M. Sorenson Brotten and Michael E. Tuttle

JANUARY 2025
The Historical Development of Public Nuisance
Zandra Foley, Stephanie Laws, Marc E. Williams, and Grant Worden

JANUARY 2025
Third-Party Litigation Funding: State and Federal Disclosure Rules and Case Law
Mark Behrens

JULY 2024
Georgia Bad Faith Alert - Holt Demands and The Case of the Missing Comma: "Caution, This Check May Self-Destruct in 90 Days"
John Lucas and Robert L. Shannon, Jr.

JANUARY 2024
Defusing Nuclear Verdicts Prior to Trial
John Lucas, Whitney Frazier Watt, and Adam J. Bobkin

DECEMBER 2023
Collision Mitigation Systems – With Innovation, Comes Litigation
Harry Byrne, Sharon Caffrey, and Ryan Monahan

NOVEMBER 2022
Unlimited Liability? Québec Tobacco Litigation And Its Ramifications For Product Liability Class Actions
Shaun E. Finn, Audrée Anne Barry, and Camille Rivard