



**The Journal of Robotics,
Artificial Intelligence & Law**

Editor's Note: Data

Victoria Prussen Spears

The European Union's Data Act

Martin Braun, Anne Vallery, and Itsiq Benizri

Artificial Intelligence and Product Liability

Joseph Mazzarella and Kimberly Castellino Metzger

The USPTO's AI Guidance on AI-Assisted Inventions and Patent Subject
Matter Eligibility

Steven L. Wood

Novel Settlement Reached in Generative AI Deceptive Trade Practices
Healthcare Investigation

Jennifer Rangel and Danielle A. Giaccio

The Impact of Artificial Intelligence on M&A Deals—Part I

Peter A. Emmi

Start-Up Corner: The Role of Different Convertible Instruments in Start-Up
Financing

Jim Ryan

- 83 Editor’s Note: Data**
Victoria Prussen Spears
- 87 The European Union’s Data Act**
Martin Braun, Anne Vallery, and Itsiq Benizri
- 107 Artificial Intelligence and Product Liability**
Joseph Mazarella and Kimberly Castellino Metzger
- 113 The USPTO’s AI Guidance on AI-Assisted Inventions and Patent Subject Matter Eligibility**
Steven L. Wood
- 121 Novel Settlement Reached in Generative AI Deceptive Trade Practices Healthcare Investigation**
Jennifer Rangel and Danielle A. Giaccio
- 125 The Impact of Artificial Intelligence on M&A Deals—Part I**
Peter A. Emmi
- 147 Start-Up Corner: The Role of Different Convertible Instruments in Startup Financing**
Jim Ryan

EDITOR-IN-CHIEF

Steven A. Meyerowitz

President, Meyerowitz Communications Inc.

EDITOR

Victoria Prussen Spears

Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

Jennifer A. Johnson

Partner, Covington & Burling LLP

Paul B. Keller

Partner, Allen & Overy LLP

Garry G. Mathiason

Shareholder, Littler Mendelson P.C.

James A. Sherer

Partner, Baker & Hostetler LLP

Elaine D. Solomon

Partner, Blank Rome LLP

Edward J. Walters

Chief Strategy Officer, vLex

John Frank Weaver

Director, McLane Middleton, Professional Association

START-UP COLUMNIST

Jim Ryan

Partner, Morrison & Foerster LLP

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at \$495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. Copyright 2025 Fastcase, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact Fastcase, Inc., 729 15th Street, NW, Suite 500, Washington, D.C. 20005, 202.999.4777 (phone), or email customer service at support@fastcase.com.

Publishing Staff

Publisher: Leanne Battle

Production Editor: Sharon D. Ray

Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Copyright © 2025 Full Court Press, an imprint of Fastcase, Inc.

All Rights Reserved.

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

729 15th Street, NW, Suite 500, Washington, D.C. 20005

<https://www.fastcase.com/>

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 729 15th Street, NW, Suite 500, Washington, D.C. 20005.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc.,
26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@
meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Leanne Battle, Publisher, Full Court Press at leanne.battle@vlex.com or at 202.999.4777

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)

ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

Artificial Intelligence and Product Liability

Joseph Mazarella and Kimberly Castellino Metzger*

In this article, the authors explore the product liability risks for products and services that incorporate artificial intelligence.

As federal agencies and states grapple with regulating artificial intelligence (AI) to enhance its safety profile, and as businesses race to adopt AI for myriad purposes, it is important to recognize that a general safety framework already exists in the form of product liability laws.

Notably, many industry experts have opined that AI systems are “black boxes” and not even their own creators are sure how they work insofar as decision logic traceability is concerned.¹ As manufacturers and sales distribution entities embrace AI and incorporate it into their products and services, they should account for and establish policies, procedures, and processes designed to limit personal injury and property damage (and the related exposure) caused by dangerous defects in products that incorporate AI.

Product Liability

Product liability is a complex area of state law relating to but distinct from legal concepts of negligence, breach of warranty, and strict liability in tort (liability without fault). Product liability may be governed by statute, case law, or both. As such, the laws and rules surrounding product liability are not uniform and can vary significantly from one jurisdiction to another. However, despite jurisdictional differences, there are common principles underlying product liability that provide a general roadmap to formulating policies and procedures that can help limit exposure for businesses in the chain of distribution of products that incorporate AI.²

The fundamental theory of product liability is that a manufacturer, seller, or other person in a product’s sale distribution chain is liable for damages when a “product” is sold to an end user or

consumer in a defective, unreasonably dangerous condition that causes physical harm to the person or their property. In the case of AI, depending on its use context (both intended and unintended), product liability becomes an area requiring careful consideration. Generally, if an AI-incorporating offering is regulated by the applicable law (e.g., is a “product” as defined by statute or case law), there are three bases that may give rise to product liability:

1. Manufacturing defects,
2. Design defects (which are often difficult to distinguish from manufacturing defects), and
3. Warnings defects.

Manufacturing Defects

Although laws vary by jurisdiction, a manufacturing defect is generally the presence of a dangerous nonconformity that deviates from product specifications or a dangerous post-manufacturing product modification by a party in the chain of distribution. In some jurisdictions, the manufacturer or seller is “strictly liable” for damages caused by a manufacturing defect, meaning the manufacturer or seller is liable to the end user even if it was not negligent.

For AI, mitigating manufacturing defects is intrinsically challenging, especially when incorporating or using third-party AI. AI models and underlying data sets can be opaque and generally cannot be interrogated at a logical instruction level to ensure that an AI system will do what it is designed to do under all circumstances for which it is designed. Unlike tangible products or traditional software employing Boolean logic, the ability to inspect an AI instantiation against its design specifications is not feasible. This is because of its complexity, hyperspace topology, probabilistic algorithms, transformations, and modularized or tokenized data constructs. Rather, model suitability is behaviorally assessed by the level of accuracy of its output.

The inability to inspect for conformity is magnified when general intelligence or deep AI is employed to perform interpretive or perceptive functions that invoke near-real-time decision making that has immediate effects or consequences in the real world. Unforeseen edge case conditions or novel situations, breadth of user adoption, and the type of activity may radically increase the magnitude of risk exposure for a business. Because of the opacity

of these systems, it raises the question whether an AI component that misbehaves in an unexpected way might be considered a design defect rather than a manufacturing defect.

Design Defects

A design defect is generally a design aspect that makes a product unreasonably dangerous. Even if a product is manufactured to specification, the product may nonetheless be defective and unreasonably dangerous because of the way it is used, could be used, operates, or functions. Some courts consider design defects as a species of negligence. Other courts do not, and unlike negligence where the manufacturer or seller may be exculpated if it did not intend and could not reasonably foresee a use that caused harm, the threshold instead is what the end user or consumer reasonably expected. Design defect liability is a complex and often subjective area and is often a matter for which expert testimony is required to show whether the product could have been designed in a safer way.

Given that AI is a relatively new product “component” and is being developed, marketed, and adopted while we are still discovering its capabilities and limitations, it remains an open question whether, for example, a deep neural network should be considered inherently dangerous as a matter of design—that is, whether the means of its internal behavior (i.e., how it operates in a conventional step transformation process) is sufficiently unknowable and uncontrollable that it renders it unreasonably or inherently dangerous, or at least unreasonably or inherently dangerous for certain types of use.

On the one hand, exhaustive testing coupled with monitoring and adequate safety controls may be sufficient to mitigate black box deficiencies.

On the other, because many AI systems enjoy plasticity (i.e., weightings, transformation functions, and topological relationships between layers can change with additional information or feedback), their adaptivity takes on an amorphous, or shape-shifting attribute.

Many businesses are likely to employ third-party AI rather than invent their own. Therefore, downstream licensees are more likely to adapt AI systems with private data models or changing various model parameters for specific uses. Doing so bears similarity to product modifications made by the distributor of a physically

manufactured product, inviting sub-tier primary manufacturing and design, or manufacturing defect exposure and providing upstream entities with defenses that the defect originated down the chain. Further, powerful AI systems allow users to use AI-powered systems or products in ways unforeseen or unintended by its developer or distributor. Thus, businesses adopting AI systems may find themselves inviting more risk exposure than may be apparent on the surface. The ability to control use and instruction becomes another important consideration in product design and leads to the third prong of product liability—failure to warn defects.

Failure to Warn Defects

Failure to warn defects arise when a product lacks appropriate instructions or warnings to enable an end user to avoid using a product in an unreasonably dangerous way. Again, because AI can be used in myriad ways, the ability to sufficiently anticipate potential uses and warn users is challenging. Generally, the more general and powerful the AI, the greater likelihood that a system will be adapted or applied (used) in unforeseeable ways. Ensuring proper user instruction and limiting an AI's use through license terms, functional governors, and exception monitoring all need to be considered.

An area that requires particular attention is the role UI/UX (user interface/user experience) plays in failure to warn. The quality, clarity, and conspicuousness of instruction, system state, action, and confirmation messaging become highly important. This is especially true where human validation is used in systems as a fail-safe mechanism in high-risk systems. Yet, it is only as effective as the UI/UX and machine-to-human communication and a human's ability to take appropriate action without delay, confusion, or mistake. In this regard, "paper" solutions such as relying on references to online acceptable use policies or user instructions may not be sufficient in themselves, and holistic system design becomes an important factor in risk mitigation.

Conclusion

Overall, businesses should appreciate that AI-based product liability litigation will undoubtedly be extremely complex due to

the black box nature of these systems. Businesses using AI in their products and services offerings need to develop a thorough risk management framework (RMF) with governance policies, procedures, and process that protect against many potential AI internal and external risks. An RMF is a complex multi-domain endeavor that includes security, data and privacy protection, licensing, insurance, indemnification, regulatory compliance, intellectual property, and a host of other considerations. However, product design, verification and validation testing, controlled in-market testing, monitoring, and remediation serve as the backbone of a sound risk mitigation framework. Product design informed by the principles of product liability law will help businesses limit unexpected exposure.

Notes

* The authors, partners at McCarter & English, LLP, may be contacted at jmazzarella@mccarter.com and kmetzger@mccarter.com, respectively.

1. See, e.g., L. Blouin, "AI's Mysterious 'Black Box' Problem, Explained," University of Michigan–Dearborn News (Mar. 6, 2023), <https://umdearborn.edu/news/ais-mysterious-black-box-problem-explained>. However, Anthropic claims to have made progress decoding the AI blackbox problem. See K. Roose, "A.I.'s Black Boxes Just Got a Little Less Mysterious," New York Times (May 21, 2024), <https://www.nytimes.com/2024/05/21/technology/ai-language-models-anthropic.html>.

2. See Restatement (Second) of Torts § 402A (1965), Special Liability of Seller of Product for Physical Harm to User or Consumer.