Volume 7, No. 6 | November–December 2024

RAIL

The Journal of Robotics, Artificial Intelligence & Law

Editor's Note: Best Practices
Victoria Prussen Spears

Three Best Practices to Mitigate High-Stakes AI Litigation Risk
Justin R. Donoho

Mastering Automated Privilege Logging: How Litigants Can Maximize Efficiency and Limit Expense
Stephen M. Medlock, Alex Rant, Michael McCambridge, and Jennifer Williams

Training Artificial Intelligence Models on Synthetic Data: No Silver Bullet for Intellectual Property Infringement Risk in the Context of Training AI Systems—Part II
Gareth Kristensen, Angela L. Dunning, Gaia Shen, Prudence Buckland, Jan-Frederik Keustermans, and Alix Anciaux

A Guide to the Federal Income Tax Treatment of Simple Agreements for Future Equity
Scott W. Dolson

European Union's Artificial Intelligence Act Is Published
Ana Hadnes Bruder and Oliver Yaros

Start-Up Corner: Choosing an Entity for Raising Venture Capital Funding in the United States
Jim Ryan

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 7, No. 6 | November–December 2024

403 **Editor's Note: Best Practices**
Victoria Prussen Spears

407 **Three Best Practices to Mitigate High-Stakes AI Litigation Risk**
Justin R. Donoho

429 **Mastering Automated Privilege Logging: How Litigants Can Maximize Efficiency and Limit Expense**
Stephen M. Medlock, Alex Rant, Michael McCambridge, and Jennifer Williams

433 **Training Artificial Intelligence Models on Synthetic Data: No Silver Bullet for Intellectual Property Infringement Risk in the Context of Training AI Systems—Part II**
Gareth Kristensen, Angela L. Dunning, Gaia Shen, Prudence Buckland, Jan-Frederik Keustermans, and Alix Anciaux

437 **A Guide to the Federal Income Tax Treatment of Simple Agreements for Future Equity**
Scott W. Dolson

453 **European Union's Artificial Intelligence Act Is Published**
Ana Hadnes Bruder and Oliver Yaros

459 **Start-Up Corner: Choosing an Entity for Raising Venture Capital Funding in the United States**
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 2024 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 © 2024 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)

European Union's Artificial Intelligence Act Is Published

Ana Hadnes Bruder and Oliver Yaros*

In this article, the authors summarize key points and recommendations for businesses using and developing artificial intelligence that potentially will fall in the scope of the EU's new artificial intelligence law.

On July 12, 2024, the EU's new artificial intelligence (AI) law (the EU AI Act)[1] was published in the *Official Journal of the European Union*. The text[2] of the law is final and entered into force on August 1, 2024, and its provisions start applying according to the staggered timeline below. This article summarizes key points and recommendations for businesses using and developing AI, that will potentially fall in the scope of the EU AI Act.

Staggered Timeline of Application

- Provisions on banned AI systems will start applying within six months of entry into force of the text—that is, by February 2, 2025;
- Provisions on general purpose AI systems will start applying one year after entry into force—that is, by August 2, 2025;
- The bulk of the obligations arising from the EU AI Act will start applying two years after entry into force—that is, by August 2, 2026; and
- Some obligations applying to high-risk AI systems that are safety components in products regulated in EU product safety legislation will start applying three years after entry into force—that is, by August 2, 2027.

Robotics, Artificial Intelligence & Law / November–December 2024, Vol. 7, No. 6, pp. 453–457.
© 2024 Full Court Press. All rights reserved.
ISSN 2575-5633 (print) /ISSN 2575-5617 (online).

Potential Impact of the EU AI ACT on U.S. and Global Companies

- U.S. and global companies that use AI anywhere could be subject to the EU AI Act if the output of the system is used in the European Union.
- For example, if a U.S. company uses an AI tool to filter curriculum vitaes for a job vacancy in the European Union, that means that the output of the AI system will be used in the European Union, and the EU AI Act will apply.
- Another example is a high-risk AI system developed in the United States and integrated into a product (e.g., in a connected vehicle) that is then sold in the European Union.
- Global companies implementing AI in their products and selling them globally would likely benefit from a global approach to AI regulatory compliance, while global companies taking a regional approach to product offering might choose to adopt regional compliance programs.
- The downside of the regional approach is that different compliance approaches might hinder the organization's ability to offer products in other regions in the future. For this reason, much like the General Data Protection Regulation set the standard in global privacy, the EU AI Act might impose itself as global AI regulatory standard and influence other AI legislation in the making across the globe.

Levels of Risk

The EU AI Act follows a risk-based approach to AI, dividing AI systems that are not general purpose AI into three main risk categories:

- Unacceptable risk, which is prohibited, such as social scoring or systems that explore vulnerabilities of specific groups of persons;
- High risk, which is permitted under the condition of compliance with strict requirements such as conformity assessments and other extensive compliance obligations (e.g., relating to cybersecurity, privacy, data governance, risk and quality management, technical documentation,

and serious incident notification). High-risk AI systems include AI systems in employment and workers' management, as well as safety systems used in civil aviation, medical devices, or critical infrastructure;
- Limited risk, which concern systems that directly interact with humans (such as chatbots), and are permitted as long as they comply with certain transparency obligations (i.e., end users must be made aware that they are interacting with a machine);
- Low risk, which concern AI systems that do not trigger any obligations under the EU AI Act. According to certain studies, many AI systems will likely fall under this category.

Different Sets of Obligations Apply Depending on the Scenario

- For each AI system being developed or used, companies will need to assess several aspects in order to determine their obligations, if any, arising from the EU AI Act:
  - What their role is with regard to the AI system (as a provider, deployer, importer, or distributor);
  - The type of AI, in particular, whether the system is general purpose AI or not;
  - For general purpose AI, whether there is systemic risk; and
  - For other AI systems, what the level of risk is (unacceptable, high risk, limited risk, or low risk).
- For example:
  - Providers of high-risk AI systems will have to conduct strict compliance obligations; and
  - In contrast, deployers of limited-risk systems like chatbots only have to comply with transparency obligations under the EU AI Act.

Impact on Technology Transactions Like the Purchasing of AI, White-Labeling, and Outsourcing

- The EU AI Act will likely help businesses purchasing AI because it will clearly stipulate which obligations fall on

providers of those systems (which will be the most extensive obligations);
- Terms and conditions of providers of AI systems will need to be amended to reflect that, and technical documentation will need to be provided by the provider of the system, and attached to the contract, so that the deployer of the system can follow any applicable instructions;
- In addition, the provider will want the contract to clarify those obligations that fall on the deployer of the system (e.g., data governance obligations if the deployer is the one in control of the data that is input into the system). So the purchasing of AI systems will likely undergo some contractual changes with the adoption of the EU AI Act; and
- Additional interesting questions relate to the allocation of obligations between providers (e.g., if an AI system is sold by a company other than the developer, under its trademark) or between deployers (e.g., in outsourcing, if a vendor of a company uses AI, and both are likely to be considered deployers). Another question is whether liability for a violation of the EU AI Act can fall on the contractual party in these scenarios.

What Businesses Should Be Doing Now

The EU AI Act will increase the scrutiny over AI systems developed and deployed in the European Union, or developed and deployed elsewhere but having an impact on the European Union because the output of the AI system is used within the European Union. Businesses developing or using AI in the European Union or with effect on the European Union, as well as investors of businesses relying on AI systems, will benefit from conformity efforts at the early stages of development or deployment of AI systems, aiming at decreasing risks and increasing trust in their systems. Recommended preliminary compliance steps include:

- Implement AI governance within the organization. There should be a body responsible for AI, as diverse as possible and including stakeholders from key parts of the business (such as development and product teams, procurement,

compliance, legal, privacy, cyber, intellectual property (IP), human resources);
- Review AI systems and use cases. The AI body should have a process in place to review AI systems and use cases, in order to assess applicable obligations under the EU AI Act, prepare for compliance with the EU AI Act (as well as other global frameworks in the making) and take into account the several AI-related risk areas (such as data/privacy, cyber, ethics, IP, etc.);
- Critically assess data governance practices for training of AI models in view of the requirements of the EU AI Act;
- Consider implementing AI policies within the organization to reflect regulatory obligations and mitigate AI-related risks;
- Prepare the support documentation of the relevant AI system in line with conformity, documentation, data governance, and design obligations; and
- Train staff on the development and use of AI to mitigate AI-related risks.

Leveraging structures and review processes in place might prove useful when implementing AI governance within organizations. For example, many global companies have processes in place when onboarding new tools from a privacy or cyber perspective, that can be leveraged for AI regulatory review as well. The AI review process can either be focused on regulatory aspects, or it can seek to address not only regulatory risk but also AI-related risks broadly (such as data/privacy, cyber, ethics, IP, etc.). Also, AI governance can take many different forms, depending on how global the organization is, its size and its development or use of AI.

Notes

* The authors, partners in Mayer Brown, may be contacted at abruder@mayerbrown.com and oyaros@mayerbrown.com, respectively.

1. EU Regulation 1689/2024.
2. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689.