



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

Editor's Note: Argumentation in AI
Victoria Prussen Spears

Argumentative Intelligence
Marc Lauritsen

Defining Autonomy in the Context of Tort Liability: Is Machine Learning Indicative of
Robotic Responsibility? Part I
Katherine D. Sheriff

Three IP Issues to Watch Out for When It Comes to NFTs
Caroline Simons, Sheryl Koval Garko, and Mark S. Puzella

Users as Digital Assets: Highlights From a Tax Perspective
Giuliana Polacco and Annarita De Carne

New Proposed EU AI Regulation Extends Beyond Europe
Justin Williams, Natasha G. Kohne, Michelle A. Reed, and Jenny Arlington

Everything Is Not *Terminator*: What Can the Law Do With AI?
John Frank Weaver

- 323 Editor’s Note: Argumentation in AI**
Victoria Prussen Spears
- 327 Argumentative Intelligence**
Marc Lauritsen
- 353 Defining Autonomy in the Context of Tort Liability: Is Machine Learning Indicative of Robotic Responsibility? Part I**
Katherine D. Sheriff
- 373 Three IP Issues to Watch Out for When It Comes to NFTs**
Caroline Simons, Sheryl Koval Garko, and Mark S. Puzella
- 377 Users as Digital Assets: Highlights From a Tax Perspective**
Giuliana Polacco and Annarita De Carne
- 383 New Proposed EU AI Regulation Extends Beyond Europe**
Justin Williams, Natasha G. Kohne, Michelle A. Reed, and Jenny Arlington
- 389 Everything Is Not *Terminator*: What Can the Law Do With AI?**
John Frank Weaver

EDITOR-IN-CHIEF

Steven A. Meyerowitz

President, Meyerowitz Communications Inc.

EDITOR

Victoria Prussen Spears

Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

Miranda Cole

Partner, Covington & Burling LLP

Kathryn DeBord

Partner & Chief Innovation Officer, Bryan Cave LLP

Melody Drummond Hansen

Partner, O'Melveny & Myers LLP

Paul B. Keller

Partner, Allen & Overy LLP

Garry G. Mathiason

Shareholder, Littler Mendelson P.C.

Elaine D. Solomon

Partner, Blank Rome LLP

Linda J. Thayer

Partner, Finnegan, Henderson, Farabow, Garrett & Dunner LLP

Edward J. Walters

Chief Executive Officer, Fastcase Inc.

John Frank Weaver

Attorney, McLane Middleton, Professional Association

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 2021 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., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff

Publisher: Morgan Morrisette Wright

Journal Designer: 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 © 2021 Full Court Press, an imprint of Fastcase, Inc.

All Rights Reserved.

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004

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

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

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, 646.539.8300.

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:

Morgan Morrisette Wright, Publisher, Full Court Press at mwright@fastcase.com
or at 202.999.4878

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)

New Proposed EU AI Regulation Extends Beyond Europe

Justin Williams, Natasha G. Kohne, Michelle A. Reed, and Jenny Arlington*

The authors discuss key elements in the European Commission's draft Regulation on Artificial Intelligence of interest to businesses.

The European Commission (“Commission”) has published its draft Regulation on Artificial Intelligence (“AI”). The draft regulation follows the strategies outlined in the February 2020 Commission’s White Paper on AI.¹

The draft regulation is of key importance to users and providers of AI, not only because it is the first attempt at comprehensive regulation of AI but also because it may well become the global standard. It is sector-agnostic, has an extraterritorial reach, carries steep non-compliance penalties and applies to multiple stakeholders across the AI value chain. The impact on business will take time to be felt, but there is already concern as to the regulatory burden. This article sets out points in the draft regulation that businesses should be aware of.

Risk-Based Approach

The draft regulation identifies four levels of risk, and it will be for businesses to identify what AI systems they use or provide, and which risk group each falls into.

Applications at the highest “unacceptable risk” level are banned. Prohibited applications include those that may materially distort the behavior of a person in a manner that causes (or is likely to cause) physical or psychological harm, and AI systems used by public authorities to evaluate and classify the trustworthiness of natural persons resulting in the detrimental or unfavorable treatment of those persons.

“High-risk” applications are not prohibited but are subject to a raft of new restrictions. Such applications include those relating to:

- Certain machinery, medical devices, civil aviation, vehicles and railways;
- Biometric identification;
- Access to essential private and public services (including issues such as evaluation of the creditworthiness of natural persons);
- Recruitment and employees’ management; and
- Management of critical infrastructure.

There is also regulation of “low/limited” risk applications, with only those with “minimal” risk escaping mandatory new obligations (for those the draft regulation includes, however, the option to adhere to voluntary codes of conduct).

Broad Scope of Activity Caught

Compliance will be made more difficult by the breadth of the proposed definition of “AI systems,” which aims to be technologically neutral and future proof. For example, it includes software that is developed with AI techniques and approaches, such as supervised, unsupervised and reinforcement machine learning; and statistical approaches, search, and optimization methods.

Wide Range of Participants Caught

The draft regulation imposes different requirements on a variety of participants in the AI value chain, and there may be scope for some uncertainty and fluidity as to which category particular businesses fall into.

The bulk of the proposed obligations are imposed on “providers” and “users” of AI, but these terms are defined broadly. Therefore, “providers” include those who develop an AI system, or have an AI system developed and placed on the market or put into service. But in addition, if any user, distributor, importer, or other third party modifies the intended purpose of a high-risk AI system, then they may be considered a “provider” and subject to the obligations imposed on providers. “User” is defined as any natural or legal

person, public authority, agency, or other body using an AI system under its authority.

In addition, other obligations are imposed on product manufacturers, importers, distributors, and authorized representatives.

In recognition of the compliance burden this will impose on businesses, some concessions are made for small and medium-sized enterprises and start-ups, including by setting up AI regulatory “sandboxes” (i.e., controlled environments to test innovative technologies for a limited time).

Extraterritorial Scope

There is extraterritorial scope. The draft regulation applies to users of AI in the European Union, and to any provider placing AI on the market or putting AI into service in the European Union, regardless of where that provider is established. Further, it applies to any providers and users of AI that are located outside the European Union, “where the output produced by the AI system is used in the EU.”

AI systems developed or used exclusively for military purposes are excluded from scope.

Requirements for “High-Risk” AI Systems

The draft regulation will impose a raft of mandatory requirements for high-risk AI systems and related obligations on providers and users as well as other key participants in the AI value chain.

These obligations include:

- Establishing a risk management system for the life cycle of high-risk AI;
- Meeting the specified quality criteria in the training and testing data;
- Creating technical documentation before the AI system is placed on the market or put into service;
- Enabling AI systems to automatically record events (logs) that must conform to certain standards;
- Ensuring transparency in the design and development of the systems so that users can interpret their output;

- Enabling AI systems to be overseen by natural persons; and
- Achieving accuracy, robustness, and cybersecurity.

Further, high-risk AI systems will have to undergo a conformity assessment, that is, a process of verifying whether the new requirements for such systems have been fulfilled. The type of conformity assessment varies depending on the AI system: it may be by way of internal control; or carried out by existing bodies for those systems that are currently regulated under other EU laws (e.g., machinery, lifts, toys, and medical devices); or by newly designated bodies, in the case of biometric identification, for example.

Certain high-risk AI systems will need to be registered (and specified information provided) in a newly created public EU database.

Requirements for “Low-Risk” AI Systems

Certain AI systems that pose “low risk” will also be required to meet new obligations, where there is a clear risk of manipulation, for example, by use of chatbots or “deep fakes.” Providers and users of such AI will be required to meet certain transparency standards to ensure that natural persons are aware that they are interacting with an AI system.

Enforcement

It is envisaged that each EU Member State will designate one or more national competent authorities, and among them one national supervisory authority, for the purposes of supervising the application and implementation of the new rules.

At the EU level, a newly established European Artificial Intelligence Board will work with the Commission to ensure that the draft regulation is effectively implemented and applied as well as assisting with new and emerging issues.

The proposed fines for noncompliance are significant: breach of certain articles may result in fines of up to six percent of annual global turnover (or €30,000,000 [approximately \$36,200,000], whichever is higher), with other breaches carrying a penalty of up

to four percent of annual global turnover (or €20,000,000 [approximately \$24,140,000], whichever is higher).

Notes

* Justin Williams, Natasha G. Kohne, and Michelle A. Reed are partners in Akin Gump Strauss Hauer & Feld LLP. Jenny Arlington is a counsel with the firm. The authors may be contacted at williamsj@akingump.com, nkohne@akingump.com, mreed@akingump.com, and jarlington@akingump.com, respectively.

1. https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.