Volume 3, No. 4 | July–August 2020

RAIL

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 3, No. 4 | July–August 2020

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. 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 Morrissette Wright
Journal Designer: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

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

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

For questions or Sales and Customer Service:

Customer Service
Available 8am–8pm 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)

EU Issues White Paper Outlining Framework for Regulating Artificial Intelligence

K.C. Halm and Jonathan Mark*

The authors review a European Commission white paper that proposes a risk-based framework for potential artificial intelligence regulations.

Less than three months after taking office, European Commission ("Commission") President Ursula von der Leyden fulfilled her promise to articulate a framework for regulating artificial intelligence ("AI"). The Commission released this framework in a much-anticipated proposal outlining potential AI regulations in its "White Paper on Artificial Intelligence (AI)—A European Approach to Excellence"[1] ("White Paper").

Together with the Commission's communications on "Shaping Europe's digital future"[2] and "A European strategy for data,"[3] these documents expand on the Commission's wider priority to create a Europe fit for the Digital Age. The White Paper presents the Commission's proposed framework for considering a formal regulatory regime applicable to AI, but does not go so far as proposing specific rules that could, or should, be adopted.

The Commission begins with a working assumption that any future regulatory framework would apply to products and services relying on AI. Without actually defining AI, the Commission references definitions previously provided in its Communication on AI for Europe[4] and by the High Level Expert Group,[5] noting that future legislation must be sufficiently flexible to accommodate technical progress while also precise enough to provide legal certainty.

To strike a balance between rules that are effective in achieving their objectives without being excessively prescriptive, the Commission urges a risk-based regulatory approach applicable to only those AI applications determined to be "high risk." The White Paper also discusses potential requirements for high-risk

Robotics, Artificial Intelligence & Law / July–August 2020, Vol. 3, No. 4, pp. 275–280

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

applications, assigning legal duties to entities in the AI ecosystem, and establishing potential enforcement and compliance regimes.

Notably, this proposed framework contrasts with many of the concepts outlined by the Trump administration in its recent policy articulating a light-touch approach to regulating AI. The Commission's AI proposals continue the EU's legacy of embracing top-down regulatory approaches to emerging technology, in the same manner as the General Data Protection Regulation ("GDPR") and other data directives.

Risk-Based Approach

Under the Commission's proposed risk-based framework, it would consider whether both the sector and intended use involve significant risk when viewed from the perspective of safety, consumer rights, and fundamental rights. Only applications meeting both "high-risk" criteria would be subject to the mandatory requirements imposed in a future AI regulatory framework.

However, applications affecting consumer rights (e.g., employment) and applications employing remote biometric identification and other intrusive surveillance technologies would always be considered "high-risk."

- *Sector*—The White Paper initially lists health care, transportation, energy, and certain public-sector functions like criminal justice and social benefits administration as uses of AI where risks are most likely to occur. It recommends that regulatory oversight be targeted to these "high-risk" sectors, which would be exhaustively listed in any future framework to be periodically reviewed and amended as necessary.
- *Use*—Acknowledging that not every use of AI in a given sector involves significant risk, the Commission proposes to assess risk based on the impact on the affected party. Such a framework would target AI applications that produce legal or similarly significant effects for the rights of an individual or a company, or that pose risk of injury, death, or significant "material" damage, such as an individual's safety, health, or damage to property, or "immaterial" damage, such as loss of privacy or human dignity, limitations

on the right of freedom of expression, or discrimination in access to employment.

Types of Potential New Requirements on High-Risk AI

Building on recommendations in the EU High Level Expert Group guidelines on AI, potential new requirements identified by the Commission include those discussed below.

Training Data

The data provided to an AI system is essential to determine a system's ultimate output. Acknowledging this, the Commission envisions requirements that are aimed at providing reasonable assurances that AI systems are trained on data sets that are sufficiently broad and cover all relevant scenarios needed to avoid dangerous situations.

The White Paper proposes that systems should take reasonable measures to ensure that the AI system does not produce outcomes that would result in unlawful discrimination (*e.g.*, gender, ethnicity), and ensure that privacy and personal data are adequately protected during the use of AI-enabled products and services.

Records and Data Retention

The Commission suggests that a regulatory framework could prescribe rules aimed at ensuring accurate records are maintained regarding the data set used to train and test an AI system. This would include a description of the main characteristics and how the data set was selected.

In certain cases, the Commission proposes requirements to maintain the data sets themselves. Additionally, the White Paper suggests maintaining documentation on the programming and training methodologies, as well as the processes and techniques that are used to build, test, and validate the AI systems—including testing for bias that could lead to legally prohibited discrimination.

While it does not propose a specific retention period, the Commission states that should be retained for a limited, reasonable time

period that will ensure effective enforcement of relevant legislation, and records should be made available upon request for testing or inspection by competent authorities while protecting trade secrets and other confidential information.

Transparency (Information Provision)

The White Paper identifies several transparency measures that would, if adopted, require developers to provide information regarding the capabilities and limitations of a given system, as well as its intended use and expected level of accuracy. It also suggests implementing GDPR-like measures to ensure that citizens are clearly informed when they are interacting with an AI system and not a human being.

Robustness and Accuracy

To ensure trustworthiness, the Commission urges that a future framework should include requirements to reflect accuracy levels during all life cycles, ensure outcomes are reproducible, and make certain that AI systems can adequately deal with errors or inconsistencies during all life-cycle phases.

AI systems should also be resilient against both overt and more subtle attempts to manipulate data or algorithms and that mitigating measures are taken in such cases.

Human Oversight

To achieve the Commission's goal of trustworthy, ethical, and human-centric AI, the White Paper urges that any proposed framework ensure appropriate human involvement in relation to high-risk applications. Such oversight could vary from conditioning that outputs of AI systems do not become final until reviewed and validated by a human or implementing a stop button or some other method to intervene in real time.

The White Paper also suggests including operational constraints in the design phase that would prevent the system from operating or controlling behavior in certain high-risk scenarios (e.g.,

programming a driverless car to stop in certain conditions of low visibility when sensors become less reliable).

Specific Requirements for Biometric Identification

The White Paper proposes to address the use of biometric information in applications like facial recognition in a separate process. Asserting that under the GDPR and other data protection and law enforcement directives, the processing of biometric data for the purpose of uniquely identifying a person carries specific risks for fundamental rights and is prohibited save for reasons of substantial public interest where the use is justified, proportionate, and subject to adequate safeguards.

The Commission does not propose to change existing law but suggests it will launch "a broad European debate" on the specific circumstances that might justify the use of biometric data for identification and related uses as well as on common safeguards.

This approach is a departure from a previous draft White Paper that proposed a ban on the use of biometric data for identification.

Assigning Legal Duties, Compliance Obligations, and Potential Enforcement Issues

In addressing the question of how to assign legal duties and obligations among the various parties involved in designing and deploying AI systems, the Commission posits that a future regulatory framework should place compliance obligations with the actor(s) who is (are) in the best place to address any potential risk. Under this approach, over the life cycle of an AI system, legal duties could shift from the developer of AI to the deployer of AI. The Commission also states its position that a future framework should apply to all relevant operators providing AI-enabled products or services in the European Union, regardless of whether they are EU entities.

The Commission proposes the use of an "objective, prior conformity assessment" to verify that high-risk AI systems meet the mandatory compliance requirements of the future framework. Although such an assessment is not formally defined in the White Paper, it would include procedures for testing, inspection, or

certification, including inspections of the algorithms and data sets used in the development phase.

The conformity assessment would be mandatory for all economic operators addressed by the requirements regardless of their place of establishment.

Voluntary Labelling for Non-High Risk AI Applications

Finally, for applications not deemed "high risk," and therefore not subject to the mandatory requirements discussed above, the Commission proposes to establish a voluntary labelling scheme. Under the scheme, interested developers could choose to conform to the mandatory high-risk system requirements or a specific set of similar requirements established for the purpose of the voluntary scheme. Those systems would be awarded a quality label, which would act as a public symbol of trustworthiness.

While participation in the labelling scheme would be voluntary, once the developer or the deployer opted to comply, the requirements would become binding. The Commission proposes that this labelling scheme would help enhance users' trust in AI systems and promote the overall uptake of the technology.

The proposals enumerated in the White Paper were subject to public consultation until May 19, 2020. The proposed legislation is expected to be released by the end of the year.

Notes

* K.C. Halm (kchalm@dwt.com) is a partner in the Washington, D.C., office of Davis Wright Tremaine LLP. Jonathan Mark (jonathanmark@dwt.com) is an associate in the firm's Washington, D.C., office.

1. https://ec.europa.eu/info/files/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

2. https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf.

3. https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.

4. https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe.

5. https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top.