Volume 4, No. 6 | November–December 2021

The Journal of Robotics, Artificial Intelligence & Law

European Commission Proposes Regulation on Artificial Intelligence

Karen L. Neuman, Hilary Bonaccorsi, Michael P. Tierney, Alec Burnside, Olaf Fasshauer, and Dorothy Cory-Wright

fastcase FULL COURT PRESS

European Commission Proposes Regulation on Artificial Intelligence

Karen L. Neuman, Hilary Bonaccorsi, Michael P. Tierney, Alec Burnside, Olaf Fasshauer, and Dorothy Cory-Wright*

This article summarizes key provisions of the European Commission's proposed regulation on artificial intelligence and offers some practical takeaways and strategic considerations for impacted organizations. Given heightened interest in AI by EU and U.S. authorities, companies will want to consider the impacts now of the proposed regulation to be well positioned—and competitive—in the regulatory environment.

On April 21, 2021, nearly three years after the EU General Data Protection Regulation ("GDPR") entered into force, the European Commission ("EC") proposed an ambitious regulation[1] establishing a framework and rules ("Proposed Regulation") for "trustworthy" Artificial Intelligence Systems. Like the GDPR, the Proposed Regulation would apply to companies located in the European Economic Area ("EEA") and third countries.

While recognizing the benefits of artificial intelligence ("AI"), the EC seeks to ensure that AI offered and used in the European market respects the fundamental rights of individuals. The EC specifically aims to protect against ethical and data privacy risks embedded in AI, including inherent bias in underlying data sets and discriminatory outcomes. Critics contend that while the Proposed Regulation creates certain initiatives[2] to promote innovation, ultimately innovation will be stifled.

This article summarizes key provisions of the European Commission's Proposed Regulation on Artificial Intelligence and offers some practical takeaways and strategic considerations for impacted organizations. Given the heightened interest in AI by EU and U.S. authorities, and the success European lawmakers have had in exporting the European privacy legal framework globally, companies will want to start considering the impacts of the Proposed Regulation now, so they are well-positioned going forward.

Robotics, Artificial Intelligence & Law / November–December 2021, Vol. 4, No. 6, pp. 433–440.

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

Background

Promoting AI built on data integrity, ethics, and security has been a focus of regulators for some time on both sides of the "pond." For example, in 2016, the U.S. Federal Trade Commission ("FTC") issued a report on "big data" in which it addressed certain risks inherent in the large data sets used to develop AI systems.[3] The EC issued a white paper in 2020 aiming to promote the adoption of AI-enhanced services, while addressing associated risks.[4]

AI remains top of mind for regulators in 2021. The FTC issued guidelines on "truth, fairness, and equity" in AI in an April 2021 blog post.[5] Some of the largest federal financial regulators, including the Consumer Financial Protection Bureau and Federal Reserve Board, issued a request for information and comment on financial institutions' use of AI in March 2021.[6]

The Proposed Regulation, however, is the first to holistically regulate a specific technology. It appears to shift to companies much of the burden of addressing systemic bias and disparate impacts associated with AI. Therefore, it will be critically important for companies to start preparing now for new obligations. Companies will also want to consider taking advantage of opportunities to shape the final version of the regulation through the legislative process.

Key provisions of the Proposed Regulation are summarized below.

Summary of Key Provisions

Common Vocabulary—Definition of AI System

AI is defined as software that is developed with one or more specified techniques and approaches (including machine learning and deep learning) that can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.

Risk Spectrum

The Proposed Regulation sorts AI uses into four risk-based categories: minimal, limited, high, and unacceptable. The primary

focus of the Proposed Regulation appears to be "high-risk" AI. High-risk AI includes:

1. Remote biometric identification of data subjects;
2. Systems known to contain bias;
3. Systems used for credit scoring; and
4. Systems used for hiring and promotion.

AI that poses a high risk would be subject to stricter requirements, including conducting conformity assessments and registering in a public registry, discussed below.

AI uses that present unacceptable risk are prohibited. These uses include AI that deploys subliminal techniques to materially distort behavior in a manner that causes the person (or another person) physical or psychological harm, exploits vulnerabilities of a specific group, or are used for social scoring or, subject to limited exceptions, for real-time biometric identification in public places for law enforcement purposes. The FTC is currently examining similar risks in its "dark patterns" initiative.[7]

Scope and Extraterritorial Reach

The Proposed Regulation applies to: (1) providers that offer AI in the EEA, regardless of whether the provider is located in or outside the EEA; (2) users of AI in the EEA; and (3) providers and users of AI where the providers or users are located outside of the EEA but the AI outputs are used in the EEA.

Conformity Assessment for High-Risk AI

The Proposed Regulation requires a conformity assessment for high-risk uses of AI. These uses will be subject to various safeguards, including transparency, functionality tests, registration, certification, monitoring, data retention, and reporting obligations. Appropriate "human oversight" will be required, as well as reporting obligations for any failure of high-risk AI that caused, or could have caused, serious injury or damage to health, safety or fundamental rights of persons concerned. While the onus for conformity assessments lies primarily on providers, that is, those introducing AI products to the European market, developers, and

others in the supply chain will also have obligations. In certain cases, a conformity certificate must be issued before an AI system can be placed in the market.

Registration

The Proposed Regulation envisions a public database for providers of high-risk AI. These AI providers would be required to register their systems before launching in the EEA. The database would contain information that would enable supervisory authorities, users, and other stakeholders to check high-risk systems against the Proposed Regulation's requirements.

Data Security and Incident Response

The Proposed Regulation requires that technical solutions for AI security incorporate measures are designed to prevent: (1) third-party manipulation of training data sets; (2) inputs designed to cause model mistake; and (3) other flaws. Trustworthy AI systems depend (almost entirely) on secure underlying data sets that developers and providers use to train and refine AI. It is critical that these data sets are secure and protected from access to or influence by unauthorized third parties. Such influence could affect AI output (regardless of industry), resulting in unintended consequences, including biased outcomes and flatly erroneous conclusions.

Oversight, Enforcement, and Fines

The Proposed Regulation would establish a European Artificial Intelligence Board ("EAIB") comprised of representatives of the EC and member states. The Board would promote the development of common AI standards and, like the European Data Protection Board, will presumably issue guidance to enable a shared understanding of the Proposed Regulation, its implementation and enforcement.

Like the GDPR, the Proposed Regulation tasks the member states with enforcement but imposes a three-tier fine regime: the higher of up to two percent of annual worldwide turnover or €10 million for incorrect, incomplete, or misleading information to

notified supervisory or other public authorities; up to four percent of annual global turnover or €20 million for non-compliant AI systems; or up to six percent of annual global turnover or €30 million for violations of the prohibitions on unacceptable AI systems and governance obligations.

Current Status and Time to Enforcement

Once the Proposed Regulation is finalized and enters into force (a process likely to run for a year or more), there will be a 24-month transition period to allow companies to implement the hefty governance, recordkeeping, and registration requirements.

What to Expect Next, Practical Takeaways, and Strategic Considerations

The Proposed Regulation must be approved by the European Parliament ("EP") and member states meeting in the Council of Ministers. We anticipate that there may be intense negotiations between the EC, EP, and member states (the trialogue process). During this process companies will have the opportunity to anticipate the Proposed Regulation's potential impact on their businesses and to educate decision makers, regulators, and the public about the implication of the new rules.

In addition, companies may want to consider taking some of the following practical steps and take into account the following strategic considerations to prepare for the Proposed Regulation.

- *Assess impact.* Those currently developing AI, or that use products that incorporate AI to perform a safety function, will want to consider core provisions of the Proposed Regulation, including its scope and global reach; robust governance and risk identification requirements related to conformity assessments, risk mitigation and management system, and governance requirements; and robust recordkeeping requirements.
- *Commit to transparency.* AI users will want to borrow from a well-established privacy policy best practice: avoid overstating the integrity of AI data or the absence of bias in AI-based personalized ads, content, products, or services.

- *Take steps to reduce bias.* Ensure that data sets used to develop and train AI include data from all populations; consider substituting proxy data for the large amounts of sensitive, protected class data required for AI, if feasible; and conduct ethics risk assessments for high-risk uses of AI.
- *Enhance security and reliability.* Take steps to ensure that AI performance cannot be altered by "poisoned" data sets or otherwise be subject to training model flaws that attackers could exploit to influence the AI decision-making processes. Use multifactor authentication, strong encryption, and state-of-the-art security measures to prevent misuse of unauthorized access to data sets.
- *Remain agile.* Despite the EC's efforts to future proof the Proposed Regulation, the final version could contain significant changes that could make the rules difficult to apply. For example, given the history of the GDPR, there is a real risk that the regulation will include derogations (escape clauses), or reserve specific powers to the member states, which could lead to partial fragmentation of the rules throughout the EEA. A potential buffer against this outcome could be for the EC to obtain buy-in by the member states for an effective certification process for obtaining the CE marker for high-risk systems.
- *Stay informed.* Be aware of evolving AI laws in other countries and industry codes across sectors. Early consideration of the potential effects of subtle, but significant nuances in other AI laws could offer tangible benefits. Many companies will recall having to retrofit their GDPR compliance (and business) strategies to address subtle obligations under the California Consumer Privacy Act.
- *Be proactive.* As noted, the Proposed Regulation suggests that the EC acknowledged limits to its ability to solve the bias and disparate effects in AI, shifting the burden for addressing these systemic effects to individual companies. There is a role for all members of society to play in eliminating these effects. A potential solution would be the creation of a multi-stakeholder entity consisting of EU and member state regulators, data scientists, industry representatives, and academics to examine the ethical effects of high-risk AI and formulate practical measures for addressing such

risks. This work could complement (not duplicate) the EAIB's standard setting and other work.

Another proactive measure could involve sector-specific collaborative efforts to help bring about the objectives that the Proposed Regulation seeks to accomplish. For example, companies may want to consider replicating the U.S. model for cybersecurity information sharing.[8] This approach could raise potential antitrust concerns. However, the U.S. Executive Branch addressed such concerns in connection with cybersecurity information sharing in a joint policy statement.[9]

Notes

* Karen L. Neuman is the co-chair of Dechert's Privacy & Cybersecurity Practice; the co-authors are lawyers in Dechert's Privacy & Cybersecurity Practice. Ms. Neuman can be reached at karen.neuman@dechert.com.

1. *Available at* https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence.

2. Pro-innovation initiatives include setting up AI regulatory sandboxes for non-high-risk AI and requiring Member States to make accommodations for and provide priority access to start-ups and emerging AI developers to create an environment that facilitates development and testing of innovative AI.

3. F.T.C., *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues* (2016), *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

4. *European Commission, White Paper on Artificial Intelligence—A European Approach to Excellence and Trust* (2020), *available at* https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

5. F.T.C., *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI*, Business Blog (Apr. 19, 2021), *available at* https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

6. Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning, 86 Fed. Reg. 16,837 (Mar. 31, 2021), *available at* https://www.govinfo.gov/content/pkg/FR-2021-03-31/pdf/2021-06607.pdf.

7. F.T.C., *Bringing Dark Patterns to Light: An FTC Workshop, News & Events* (Apr. 29, 2021), *available at* https://www.ftc.gov/news-events/events-calendar/bringing-dark-patterns-light-ftc-workshop.

8. *See, e.g.*, Exec. Order No. 13691 (Feb. 13, 2015), *available at* https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

9. *See* U.S. Dep't of Justice and F.T.C., *Antitrust Policy Statement on Sharing of Cybersecurity Information* (Apr. 10, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/04/ftc-doj-issue-antitrust-policy-statement-sharing-cybersecurity.