U.S. CHAMBER OF COMMERCE

U.S. Chamber of Commerce Comments concerning the European Commission's Proposed Artificial Intelligence Act August 6, 2021

The U.S. Chamber of Commerce welcomes the opportunity to comment on the European Commission's *Artificial Intelligence Act* ("Act" or "AI Act).

The Chamber is the largest business advocacy organization in the world, operating in all 50 states and in over 50 countries to promote free enterprise and advance American trade and investment globally, representing companies of every size and from every sector, working with state and local Chambers and over 100 AmChams around the world. The Chamber is a longtime advocate for stronger commercial ties between the United States and the European Union. According to an annual study jointly commissioned with AmCham EU, the U.S. and the EU are together responsible for one-third of global gross domestic product and transatlantic trade and investment supports 16 million jobs on both sides of the Atlantic.[1] The Chamber is also a leading business voice on digital economy policy, including on issues of artificial intelligence ("AI"), data privacy, cybersecurity, digital trade, and e-commerce. In the U.S., Europe, and globally, we advocate for sound policy frameworks that support economic growth, promote consumer protection, and foster innovation.

The Chamber believes in AI's potential as a force for good to tackle challenges such as the COVID-19 pandemic and to spur economic growth for the benefit of consumers, businesses, and society. In 2019, we issued ten principles for policymakers considering action on artificial intelligence:

1. Recognize Trustworthy AI is a Partnership
2. Be Mindful of Existing Rules and Regulations
3. Adopt Risk-Based Approaches to AI Governance
4. Support Private and Public Investment in AI Research and Development
5. Build an AI-Ready Workforce

[1] https://www.uschamber.com/sites/default/files/transatlanticeconomy2021_fullreport_lr.pdf

6. Promote Open and Accessible Government Data
7. Pursue Robust and Flexible Privacy Regimes
8. Advance Intellectual Property Frameworks that Protect and Promote Innovation
9. Commit to Cross-Border Data Flows
10. Abide by International Standards

We hope these principles serve as a guidepost for the European Commission as it engages with the European Parliament, the European Council, and stakeholders on this important piece of legislation.

The Need for Transatlantic & International Regulatory Cooperation

The Chamber welcomes the launch of the U.S.-EU Trade and Technology Council earlier this summer, which includes a working group focused on technology standards cooperation, including artificial intelligence.[2] This forum will be important to increase transatlantic collaboration and investments in critical and emerging technologies, as well as foster cooperation. Effective stakeholder and legislator dialogues are essential to achieve this. The AI Act can advance transatlantic cooperation and regulatory interoperability between likeminded, democratic market economies. The Act should direct member states, national competent authorities, and the European AI Board to engage in dialogues with democratic partners, such as the United States, to advance interoperable approaches to AI governance and create a common understanding of a trade/economic impact analysis for this work. Also, adherence to technical regulations and standards and corresponding conformity assessment procedures that are non-discriminatory and do not create obstacles to trade in accordance with WTO obligations will be critical to support transatlantic cooperation.

These efforts will minimize the risk of unnecessary regulatory divergences and trade-restrictive practices from emerging in the transatlantic digital economy. Indeed, the United States' *Guidance for Regulation of Artificial Intelligence Applications* includes such a directive. The Organization for Economic Cooperation & Development's *Recommendation on Artificial Intelligence* and groups of likeminded nations, such as the

[2] https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/15/u-s-eu-summit-statement/

Global Partnership on Artificial Intelligence, serve as important reference points in this respect.[3]

Refining the Definition of AI and Scope

The definition of AI and the list of techniques and approaches in Annex I give the Regulation a very broad scope that covers a significant amount of software applications which are not considered to be AI systems (for example, statistical approaches and search and optimization methods which have been used in many applications across industries for some time and are generally not considered AI). The definition should be refined since an overly broad approach would require more frequent updates to include new AI techniques not currently listed in Annex I (as is acknowledged in Article 4).

Given the statement in Recital 6 that "AI systems can be designed to operate with varying levels of autonomy," the concept of 'autonomy' should be included within the definition since it is a fundamental part of an AI system.

Similarly, the AI Act should be more explicit regarding the allocation of responsibilities when it comes to general purpose tools which users develop into AI systems. The text should clearly mention that when a user develops a general-purpose tool into an AI system for a high-risk intended use, it is up to the user to comply with the requirements for high-risk systems.

Refining the Risk-Based Approach

The Chamber commends the Commission on embracing a risk-based and proportionate framework for governing AI applications, which the Chamber called for in earlier comments to a *White Paper on AI: A European Approach to Excellence and Trust.* [4] We also welcome the Commission's thoughtful approach to providing a limited and narrow list of high-risk AI applications. At the same time, the EU should pay careful attention to refining, clarifying, and streamlining this framework – including clarification of commercial applications vs. in-house developed optimization technologies – rather than pre-judging products as high-risk. The Chamber works on behalf of a diverse set of members, and we encourage effective, transparent,

[3] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
[4] https://www.uschamber.com/series/above-the-fold/our-response-europe-s-ai-proposals

accountable, and consultative regulatory processes, particularly as they relate to the process by which an application is classified as high-risk. To support innovation across the EU, it is critical that high-risk AI systems are defined in ways that provide clarity to industry and protect individuals. The Act should also recognize the important benefits that responsible AI can offer for public safety, coupled with appropriate provisions to protect fundamental rights. We therefore welcome the proposed narrowly defined exceptions that the Act would allow for the use of real-time remote biometric identification in publicly accessible spaces for the purposes of law enforcement. Potential risks from such use can be effectively mitigated with appropriate safeguards, for example through clearly defined processes and controls such as human review, judicial supervision, clear use policies, reasonable boundaries around data retention, and transparency measures.

The Act should clarify that instances affirmed to be high-risk are limited to those where AI is used to make explicit recommendations or decisions (as opposed to support systems or those that are related to the high-risk activity but do not impact fundamental rights). Similarly, the proposed definition of what constitutes a "safety component" should be clarified to avoid legal uncertainty. The Act should specifically clarify the criteria for companies to demonstrate "critical use."

Lastly, sector-based safety regulators in the EU should be allowed to conduct detailed risk assessments of components – on a case-by-case basis in accordance with existing guidelines for each product submitted – to determine if any mandatory requirements for high-risk AI applications should be applied to specific products.

Avoiding Burdensome Data Governance Requirements

The AI Act would impose a long list of obligations on AI products and services deemed high-risk, including requirements on testing, training, and validating algorithms, ensuring human oversight, and meeting standards of accuracy, robustness, and cybersecurity. The costs to meet the proposed requirements are significant and may in some cases prove prohibitive. According to an independent study sponsored by the Commission, businesses would need as much as €400,000 to set up a "quality management system."[5] Few startups or small and medium-sized businesses can pay this price of admission into the AI marketplace, let alone the additional costs associated

[5] https://digital-strategy.ec.europa.eu/en/library/study-supporting-impact-assessment-ai-regulation

with compliance, thereby stifling innovation. Indeed, the AI Act would eat up as much as 17 percent of AI investment in Europe.[6]

To avoid imposing disproportionate cost requirements – particularly onto Europe's startups and small and medium-sized businesses – we also recommend rethinking the Act's data governance requirements along more pragmatic lines. AI is still in its infancy, and onerous data, technical, and transparency requirements could potentially limit the transformative potential of AI technology to address critical issues like public health, the environment, and economic recovery. While some sectors already have standards for AI governance, others lack clear and practicable consensus standards.

In order for these regulations to be effective in protecting fundamental rights while also laying a foundation for a new era in European innovation, they need to be both clear and flexible. The Act specifically calls for training and testing data to be "complete" and "free of errors," which is technically infeasible.[7] No data set can ever be complete, and the best AI systems can be robust and accurate even when there is error in the data sets. Supervised learning which utilizes human-labeled data sets will never be error-free because it is impossible to have completely unambiguous categories which human labelers will agree upon. A regulation requiring the absence of error would similarly extinguish the most promising advancements in unsupervised learning, where a key factor is the ability to use data sets that are too large for humans to manually curate. The mandate that personnel "fully understand the capacities and limitations of the high-risk AI system" are similarly unreasonable.[8]

We encourage European policymakers to work collaboratively with experts from industry to ensure an appropriately balanced approach.

Lastly, concerns regarding human accuracy are why the Chamber opposes requirements for human oversight of AI in final products and goods covered by existing regulations which require approval of products by the Commission (e.g. General Safety Regulation, Machinery Directive, etc.). Instead, the AI Act should only require human oversight when AI is used to train such systems and provide evidence of such oversight to sector-specific regulators during the approval process as appropriate.

[6] https://www2.datainnovation.org/2021-aia-costs.pdf
[7] AI Act, Article 10
[8] AI Act, Article 14.

Technology Neutrality

The AI Act should be technology neutral. It should focus on outcomes rather than specific techniques used, as this more effectively addresses underlying behaviors or practices and ensures that the legislation is future-proof. Given the speed of technological advances, technology-specific regulation will struggle to maintain pace with developments in its use and risks, creating barriers to adopting new and innovative technologies.

Concerns Regarding Access to Intellectual Property, Including Source Code, Algorithms, and Data Sets

As written, the AI Act grants regulators "full access" to enterprises' data sets and, under similarly broad conditions, access to an AI system's source code.[9] While there may be precedent for this practice in certain limited circumstances, this is a broad regulatory authority without important safeguards. At best, these actions will expose valuable intellectual property, trade secrets, and personal information to cyberattacks. The experience of the European Medicines Agency and other recent information security incidents demonstrate that regulators are prime targets for cyber criminals seeking the assets of cutting-edge technologies.[10] Businesses attempting to develop and deploy AI applications may choose to avoid the single market if valuable data are exposed to these risks. We recommend removal of these provisions in favor of a regulatory approach that recognizes the proprietary nature of this information and focuses on assessing and testing the outcomes of AI systems, as opposed to their inputs.

Additionally, we encourage clarification on the requirements to disclose data across the manufacturing applications. As written, the Act seems to extend to products manufactured with AI applications. Given that final products already have health, safety, and environmental production standards, this would be discriminatory and unnecessary. Disclosure requirements should be limited to the application technology.

[9] AI Act, Article 64

[10] https://www.reuters.com/article/us-eu-cyber/russian-chinese-hackers-targeted-europe-drug-regulator-newspaper-idUSKBN2AY0F1

If this requirement cannot be eliminated entirely, we strongly urge limiting access to such valuable intellectual property to only the extent necessary for an investigation into the most serious and compelling of circumstances for public safety and national security and to the imposition of rigorous data protection and data retention rules. In any case, source code should remain excluded from the limited access. Requests for such valuable information should be drawn as narrowly as possible to minimize the data exposed and should include appropriate safeguards: Authorities should be entitled to keep this information only for as long as it is absolutely necessary for the underlying investigation; its reproduction and circulation should be strictly prohibited; the information should be irreversibly, securely, and completely destroyed as soon as possible in the investigation; and procedures and rules should be imposed to prevent the information from being released to the public in the course of investigational and/or enforcement action proceedings.

Recommendations for a Compliance & Enforcement Regime

The Commission proposes a conformity assessment requirement for AI applications designated as high-risk. The Commission rightly acknowledges that "the AI sector is very innovative and expertise for auditing is only now being accumulated." We commend the Commission for using self-assessments for the most high-risk AI systems. Requiring prior approval for all high-risk systems would be harmful to innovation. We also agree that for products already subject to conformity assessments, especially those subjects to sector-specific safety regulations (e.g. automotive), AI risks should be assessed as part of existing conformity assessment regimes instead of a new and separate assessment process.

EU AI policies, procedures, and regulations should promote international alignment and interoperability with industry-backed approaches to risk management to the maximum extent possible. The Chamber encourages the Commission to leverage public-private partnerships to develop policy by incorporating consensus-based standards, available accreditation schemes, and globally recognized practices to meet EU compliance interests. By working with the private sector and standards bodies, government agencies can promote transparency, leverage private sector resources, contribute to economic and job growth, and give current and evolving meaning to concepts used in the regulation like data quality, transparency, accuracy, and

robustness. As the Commission contemplates the establishment of conformity assessment regimes for high-risk AI systems, the Chamber strongly urges the Commission to: (1) Build on and not duplicate existing frameworks, sector-specific regulations, and best practices; (2) Promote the voluntary use of conformity assessment and certification schemes; (3) Consider alternatives, appropriate to the risk profile, to third-party assessments such as self-assessment, vendor attestations, or accreditation of third-party assessors as a means to build and maintain confidence in conformity assessment bodies.

Regulated Entities Should Have a Substituted Compliance Model

The Commission should ensure that horizontal initiatives, such as the AI Act, do not duplicate existing requirements within sectors. For example, wholesale financial services firms are already highly regulated, including in a range of areas that are relevant to the use of AI (such as consumer protection, model risk management, conduct risk, duty to clients, internal governance, third-party risk management, technology, outsourcing, operational resilience, and data privacy). We encourage the consideration of a substituted compliance model wherever relevant requirements already exist.

The Need to Avoid Regulatory Fragmentation

Under the current proposal, member state governments can designate an array of "supervisory authorities," "notifying authorities," and "market surveillance authorities" Each member state would be required to build expertise to understand and regulate state-of-the-art technologies, and the Act would impose no obligation on these bodies to coordinate how they interpret and enforce Europe's new AI rules. AI governance frameworks should recognize the diversity of AI applications and, wherever possible, leverage existing rules and regulatory bodies. A fragmented member state-specific regulatory approach that envisions creation of a series of new institutions would slow and suppress future innovation in AI applications, discourage investments, lead to uncertain and potentially contradictory regulatory processes and outcomes, and substantially limit the benefits resulting from this powerful new set of technologies and applications.

We urge the Commission to learn from the experience of the General Data Protection Regulation's (GDPR) implementation. A major aim of the GDPR was to establish a unified data protection regime for the European Single Market. Consistent application of the Regulation by member states, together with coordinated interpretation and efficient enforcement by data protection, are necessary to realize this aim. Unfortunately, divergent and in some cases conflicting guidance from DPAs on core aspects of GDPR is inhibiting companies' ability to comply and resulting in serious unintended consequences. Similarly, GDPR's one-stop-shop mechanism promised to ease the administrative burden for companies with a pan-European footprint by enabling them to designate a lead supervisory authority when engaging in cross-border processing. While concerns have been raised about the practical implementation of the GDPR one-stop-shop mechanism, the AI Act does not propose any such coordinating function.

We suggest that competent authority supervision be established on a subject-matter basis. Furthermore, to achieve harmonized application of this regulation across the EU, opinions and recommendations issued by the European Artificial Intelligence Board on the application of this regulation should be binding for member state authorities, which should adopt them in their own acts. Regardless of the supervision model chosen for the final text of the Act, we would also note the importance of supporting supervisors in upskilling in this highly technical subject area. Supervisors must keep pace with their industries, where there is often already a high demand for technical skills, to provide effective oversight and challenge.

Concerns Regarding Disproportionate Penalties

As with the GDPR, the AI Act rightly aims to protect EU citizens from violations of applicable rules. Yet the proposed law envisions extraordinary penalties based on worldwide turnover. We believe any penalties related to a violation of the regulation should be based instead on EU revenues. This is particularly appropriate for the AI Act, which takes a risk-based approach in order to prevent harm. Using a worldwide turnover as the basis for the AI Act's penalties results in an inappropriate extraterritorial effect that extends beyond the risk that the regulation is meant to address. Such extraordinary penalties also would violate the enforcement principles of proportionality, permitting the imposition of penalties well beyond what

is justified by a company's European presence, its European revenues, and harm to individuals in the EU.

Conclusion

The U.S. business community is proud of its longstanding and substantial contributions to the transatlantic commercial relationship, and the Chamber appreciates thanks the opportunity to provide these comments. We stand ready to be part of the solution as Europe strives to build a robust digital economy, and we look forward to continuing the dialogue on the AI proposal and other important digital policy issues.

Contact

Abel Torres
Senior Director, Center for Global Regulatory Cooperation
atorres@uschamber.com
EU Transparency Register: 483024821178-51