AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Consultation response

Artificial Intelligence Act

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €3 trillion in 2020, directly supports more than 4.8 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Introduction

AmCham EU commends the European Commission for the extensive consultative process that led to the publication of the Proposal for an 'AI Act'[1]. We appreciate having had the opportunity to provide our perspective on this important piece of legislation. We provided input to the AI White Paper consultation[2] and the Roadmap consultation[3] in 2020 and are pleased that some of the points and recommendations we made are reflected in the AI Act.

The AI Act is the first attempt to lay down a comprehensive legislative framework for the development and use of artificial intelligence and the proposal will no doubt to some extent serve as an anchor for policy proposals in other countries and regions. We support the Commission's stated objectives of creating an ecosystem of trust and an ecosystem of excellence and to ensure that the EU becomes a vibrant hub for research, development and innovation in trustworthy AI applications.

We offer the following initial observations on the AI Act proposal in order to help strike the right balance between the Commission's dual objectives. We aim to highlight areas in which we see potential for clarifying and improving the proposal.

Definitions

As the first legislative proposal on AI anywhere in the world, the AI Act contains a number of concepts that have never been defined in law. AmCham EU has previously argued that it is essential to define the concept of Artificial Intelligence clearly and precisely. The definition given in the AI Act, while based on the OECD definition[4], is significantly broader than that and could encompass techniques and software that do not perform functions normally associated with AI. A similar issue goes for software that has AI capabilities built in, but is not an AI system itself per se. The definition of AI should be tightened up in order to ensure legal clarity and predictability. Clarifying definitions would contribute to legal certainty, consistency and predictability.

Recital 60 recognises the complexity of the AI value chain, made of 'relevant third parties, notably the ones involved in the sale and the supply of software, software tools and components, pre-trained models and data, or providers of network services.' The broad definition of 'AI system' and subsequently of a 'provider' makes it hard to effectively determine which AI systems and which entities (providers) would be in scope of the proposed Regulation. For this reason, we suggest the proposed Regulation clarifies the differentiation of roles across the AI value chain so that entities developing toolkits, software libraries, etc are not considered 'providers.' This could be done by stipulating that these relevant third parties are not considered 'providers of AI systems' as defined by the proposed Regulation.

A number of other definitions should be clarified: the definition of 'safety component of a product' is too broad and could cover virtually any component of a regulated medical device. There is a lack of clarity of the terms 'placing / making available on the market' and 'putting into service.' In the context of Article 9 it is not clear whether there is any difference between: (1) 'reasonably foreseeable' risks (Art 9[2][a]) and 'risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse' (Art 9[2][b]).

To reduce the ambiguity of the definition of 'safety component', we believe it is important that the assessment of a safety component refers back to EU harmonised legislation to align with any relevant essential requirements. In other words, when assessing an AI system for the purposes of paragraph 1 of Article 6, a safety

[1] Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts, Com (2021) 206 Final, Of 21 April 2021

[2] https://www.amchameu.eu/system/files/position_papers/ai_consultation_14_june_2020_final.pdf

[3] https://www.amchameu.eu/system/files/position_papers/ai_ethics_and_legal_amcham_eu_final.pdf

[4] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

component is to be understood in the meaning of the relevant Union harmonisation legislation listed in Annex II.

Finally, in relation to Article 9, the Proposal offers no guidance on what specific risks need to be taken into account by the risk management system required by Article 9. While several recitals (eg, Recitals 27, 43) indicate that the goal of the Regulation is to mitigate risks to 'health, safety and fundamental rights,' Article 9 itself does not specify the types of risks providers should consider when assessing and taking steps to mitigate risks.

Prohibited uses

Some conceivable uses of AI may cause unacceptable risks to fundamental rights and we agree with the Commission's approach to prohibit them. For example, the use of generalised social scoring systems seems difficult to justify. Banning these types of use scenarios can help address legitimate concerns about irresponsible and harmful uses of AI in European societies.

The potential use of real-time biometric identification systems in public spaces raises serious fundamental rights concerns but is allowed in the proposal under certain circumstances. If legislators decide to provide for the use of real-time biometric identification in the final AI Act, it would be important to ensure clarity about under what criteria it can be used and ensure that those who deploy it are subject to robust transparency requirements.

High-risk focus

AmCham EU is pleased to note that the stated focus of the AI Act is mitigation of actual risks associated with deployment of AI systems in particular scenarios. The focus needs to be on use scenarios where decisions rendered by AI systems can have significant impact on fundamental rights or cause health and safety concerns. The definition of high risk should also take into account human oversight: AI systems which only produce recommendations should not be considered high risk. It is appropriate to base risk assessment on particular use cases rather than designating classes of applications or sectors as inherently high-risk. For example, the classification of all HR applications as high-risk does not recognise the need to differentiate between applications in the area of HR according to actual risk. A wholesale categorisation risks stifling innovation. The definition of high-risk use cases should be tightened and clarified to ensure that only those systems that create substantive risks are captured.

The list of high-risk AI systems is excessively broad in at least two respects. First, as discussed above, the definition of 'safety component of a product' is too broad and, secondly, the list of 'high-risk' systems in Annex III is too broad and may sweep within scope systems that are neither inherently high-risk nor involved in the decision-making function of the final system (ie, the point at which a risk of harm may materialise). This is particularly the case for component parts of larger systems and general-purpose systems that may be used in a wide range of contexts. Furthermore, although Article 7(2) lists several criteria that the Commission must take into account when evaluating whether to add any new categories of AI systems to Annex III; Annex III currently could cover AI systems that would not appear to qualify as high risk under those criteria (eg, an AI system that helps manufacturers determine the number of employees needed to perform certain tasks). The Commission should consider narrowing down the list of AI systems in Annex III so that they only encompass AI systems that pose systemic 'high risks' to natural persons that interact with them.

Regulatory structure

The AI Act is conceived as a horizontal piece of legislation. It covers AI systems deployed in any industry sector and for any purpose and applies to high-risk AI systems in the New Legislative Framework[5]. This framework has been in place for some time to mitigate health and safety risks risk that could be associated with physical products placed on the European market. The AI Act brings stand-alone software into this regulatory framework

[5] https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en

and treats health and safety risks as well as risks to fundamental rights in the same way. There are good reasons for taking a horizontal approach rather than a sector- or use case-specific approach and for many types of products that embed AI systems, the regulatory and compliance structures already exist. On the other hand, applying a product safety framework to standalone software applications is likely to cause difficulties in some scenarios and may require some adjustment of the text.

It is questionable whether the same requirements designed for product safety will indeed result in the protection of fundamental rights. The proposed market surveillance approach may make sense with respect to mitigating health and safety but is likely to work less well regarding risks to fundamental rights (eg, would a discriminatory decision to deny a loan provide a basis for authorities to order the withdrawal of the system from the market?). Fundamental rights risks in relation to stand-alone AI systems would be better addressed through risk management systems by the provider, combined with appropriate transparency and accountability mechanisms by the user.

Requirements for high-risk AI systems

The AI Act lays down a list of requirements that AI systems categorised as high-risk must meet. These requirements - such as risk management, data governance, human oversight, robustness and accuracy - are on the whole sensible and in keeping with the Commission's preparatory work. However, some of the requirements seem to be overly prescriptive and detailed while some seem to be unrealistic. This is the case with the requirement for datasets to be 'free of error' and 'complete' (Article 10). The instructions to users and requirement that human oversight enable the user to 'fully understand the capabilities' of the systems seem unreasonable and probably not very useful to the user. While requirements for high-risk AI systems should be substantive and meaningful in order to create trust, they should be framed in a way that is flexible and realistic. Stringent and prescriptive requirements could result in a regulatory burden that would hamper innovation, entrepreneurship and take-up without building trust and confidence. For example, the technical documentation requirements (Article 11, Annex IV) and the transparency requirements (Article 13) are extensive and potentially overly burdensome for providers, while it may not be possible for the provider to 'enable' users to 'fully understand[s] the capacities and limitations' of a high-risk AI system as Art. 14(4)(a) requires.

In general, the AI Act should focus instead on desired outcomes in accordance with the nature of the AI system in question allowing providers discretion in achieving them.

Conformity assessment

AmCham EU supports the principle of self-assessment and declaration of conformity for high-risk AI systems. This system works well in a wide range of sectors already and enables companies to bring products to the market in a timely manner. It is essential that this principle is maintained as the European Parliament and Council consider the proposal. Were high-risk AI systems to be subject to prior assessment by third parties, it would cause a significant delay in product launches, and slow down uptake of AI applications in the public and private sectors.

Some provisions should be clarified to ensure legal certainty and create the right conditions for innovation. Articles 19 and 43 require providers to subject their systems to a new conformity assessment whenever they are 'substantially modified' (Art. 43[4]). Despite the definition of 'substantial modification' in Article 3(23) — one that 'affects' the system's compliance with the Regulation or modifies its intended purpose — it is not clear what specific actions would trigger a new assessment. On a conceptual level, this procedure presumes that there is a point in time where providers can 'freeze' the system and assess whether it is in conformity, with only 'substantial' changes warranting a reassessment. In practice, AI systems — particularly those offered as services — require constant monitoring, tweaking and adjusting throughout their entire lifecycle. Providers might find it extremely challenging to assess at what point such minor improvements over time result in a 'substantial modification' to the system.

The Proposal exempts high-risk AI systems that 'continue to learn' from having to undergo a new conformity assessment when changes occur, provided that those changes were 'pre-determined by the provider' in the initial conformity assessment and are stated in technical documentation. Greater clarity is needed on this point, because all AI systems — at least those offered as services — are arguably designed to 'continue to learn' throughout their lifecycle, so it may be worth proposing that this be made a general exemption.

Obligations on providers / users

The AI Act places most of the obligations for meeting the requirements for high-risk AI systems on providers of such systems. Users (ie customers) that deploy AI systems are required to follow instructions given by the provider for the intended use. This allocation of responsibilities is drawn from product regulation frameworks, based on the assumption that a product is sold and delivered to a customer with instructions for use. For many AI use cases, the distinction between provider and user roles is less clear than that. In many scenarios, providers create applications that are general-purpose and not high-risk. However, these same applications can be configured by users who will also control the data with which the AI system interacts. In such contexts, the provider has little or no control over and visibility on the use of the AI system and there may be a need for a different allocation of responsibilities than is foreseen in the AI Act.

In some cases, it could be relevant to place certain obligations on the user from the outset. The Regulation should also enable providers and organisational users of AI systems to contractually allocate their responsibilities. Following this approach would also make sense from the perspective of putting the obligations on the party that could most easily follow them and, from the perspective of fundamental rights, where those affected by a high-risk AI system could seek remedies from the user rather than tracing the system all the way back to its provider. Article 28 on the obligations of third parties including users applies only to systems that are already high-risk systems before they are modified by the user. Article 28 should be amended so it applies to users who modify the intended purpose of an AI system already placed on the market or put into service to create a high-risk AI system.

Transparency is critical to building trust. Transparency requirements should be targeted and provide the user or natural person with the opportunity to make an informed decision. For example, some interactions with AI systems via email do not merit notification; while it is necessary for AI systems developed to converse or communicate with people in real time.

Governance and enforcement

The AI Act foresees a complex regulatory infrastructure to oversee and regulate AI systems - from assessment and declaration of conformity to ex-post market surveillance - in line with the New Legislative Framework. Member States have considerable leeway to set up regulatory authorities as they see fit and to take into account national administrative structures. This means that it is not quite clear how responsibilities will be divided among the various authorities that already exist and that will be set up according to the requirements of the AI Act. Further, the proposal allows for significant fragmentation as Member State regulators have the authority to demand removal of AI systems from the market if they consider that there are risks associated with them. Regulators are given this authority even for AI systems that are in full compliance with all the requirements in the AI Act. The EU institutions must consider options for creating legal certainty and predictability as well as to minimise regulatory overlap and ambiguity. Regulatory coherence and coordination will also be important in the international context.

The AI Act provides for very extensive powers for market surveillance authorities to access data and documentation from providers and users of AI systems. In particular, they can compel providers of AI systems to grant access to data sets via application programming interfaces and they can request access to the source code of the AI system. These access requirements seem disproportionate and could compromise intellectual property and trade secrets as well as the security of the large amount of data that providers are obliged to retain under the AI Act. It is not consistently clear how this Act integrates with the General Data Protection Regulation as it relates to the processing of sensitive data. EU policy makers should consider more reasonable and

proportionate ways to ensure market surveillance authorities can obtain the information they need. Providers should have the right to challenge the necessity and proportionality of access requests before an independent court and should not be required to violate EU, Member State or applicable third-country laws in providing such access. Furthermore, in some cases (eg, where a provider has licensed the relevant dataset for a period of time), the provider might not retain control over the dataset over the life of the AI system at issue.

Measures in support of innovation

Of the 85 articles in the AI Act, three aim to support innovation, doing so by providing for 'regulatory sandboxes'. These are intended as controlled environments where providers can develop and test AI systems, presumably under supervision by regulatory authorities.

In general, the best way to safeguard innovation would be to ensure that the regulatory and compliance burdens the AI Act creates are manageable and the requirements are realistic. This will be especially important for European small- and medium-sized enterprises and start-up companies that need to grow and scale rapidly and whose success is critical to the future competitiveness of the European Union.