Coalition of Services Industries
Comments on
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
European Commission, EU-TBT Enquiry Point
February 2022
G/TBT/N/EU/850

The Coalition of Services Industries (CSI), based in Washington, D.C., has represented the interests of the services sector since 1982, shaping policies to facilitate the growth of services trade and promoting greater awareness of the role of services in the U.S. economy. Our members include companies and associations that provide information and communication technology services, financial services, express delivery and logistics, media and entertainment, distribution, retail and professional services.

***

Thank you for the opportunity to provide comment.

We encourage EU policymakers to more precisely define AI, as the current definition is so broad that it could be considered to encompass traditional software. Although it is important to employ a definition that can adapt to new technologies over time, the existing language is overly general.

Also, general purpose tools that are not AI systems per se, but rather serve as components or precursors of AI systems, should be excluded from the scope of the Act.

High-risk AI systems must be defined in ways that provide clarity to industry and protect individuals. Systems classified as "high risk" are subject to significant heightened compliance and oversight and, as such, the "high risk" group should be appropriately limited only to those use cases that clearly affect the fundamental rights of persons. Taking a broad approach to such classifications not only conflicts with the EU's principles on proportionality but also risks disincentivizing industries from using a tool that provides customers with better products, more personalized customer experience, reduced fraud, among other benefits.

The law should provide more clarity on how Annex 3 will be updated and on the format for stakeholder consultation related to revisions of the annex. Lack of clarity regarding any expansion of the definition of high risk is likely to deter and delay investment in technology in service industries.

Currently, the AI Act places most of the responsibility for complying with its obligations on "providers" of high-risk AI systems. This distinction ignores the complex realities of the marketplace. Depending on the situation, an AI system could be developed entirely by one party, but it may also encompass AI tools purchased from multiple vendors and patched together by a systems integrator or the user's employees. Likewise, training data may be obtained by a user internally, or from vendors. Ultimately it will in many cases be the entity that actually deploys an AI service that determines both the intended use of the final AI system – including whether to use the system in one of the high-risk scenarios listed in Annex III—and the societal context in which the system operates.

The deployer will also often be the only entity with full visibility into the system's operation and whether all relevant risks have been appropriately mitigated. Accordingly, it is appropriate that deployers of such AI systems assume responsibility for addressing those risks that are within their control. The text of the law should be revised to acknowledge this reality instead of focusing largely on providers.

Article 5 of the proposed AI Act identifies several prohibited AI practices. It is important that prohibited forms of AI be clearly and narrowly defined in order to ensure that the regulation does not prohibit a variety of other, less risky uses of AI. The penalties for bringing a prohibited AI to market are so significant that any ambiguity in those practices could chill many potentially beneficial and innovative uses of AI. As a case in point, one of the prohibited practices includes "subliminal techniques." What "subliminal" means or what it means for such a technique to "materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm" is unclear. Both terms need to be narrowly and clearly defined.

The requirement that data sets be "free of errors and complete" in Article 10 is an impossible and unrealistic standard.

Supervised learning relies on large quantities of human-labeled data. Even if it were possible to define completely unambiguous categories, any human-driven process is likely to involve mistakes. Moreover, in many of the most important circumstances (for example, identifying hate speech online) it is impossible to have completely unambiguous categories, meaning that even the most expert human labelers will disagree and make mistakes. An error free standard would make supervised learning impossible.

Unsupervised learning does not use human-labeled data, but is instead a machine learning approach that iteratively looks for patterns in large, unstructured data sets. This process is by

definition imperfect. An error free standard would foreclose some of the most promising and exciting advancements in AI research.

Because no data set can ever be error free, they are designed to operate robustly when they encounter imperfect data. For that reason, the focus on error free data is misplaced; it is more important to focus on the overall impacts of the system as a whole.

Likewise, it is not possible to create a “complete” dataset even when working to ensure key groups are represented, because there is always more data that can be collected. Among other reasons, this is because the world in which we live is ever-changing and so too is its data trail.

Also, the requirement in Article 14 to put in place human oversight that enables the user to "fully understand the capacities and limitations of the AI system” is not possible to achieve in practice, since a developer cannot guarantee what a user will understand.

The AI Act also duplicates, and potentially conflicts with, existing laws. For example, the AI Act overlaps significantly with the GDPR (such as the rights related to automated decision making and requirement to appoint EU representatives for non-EU companies). Both regimes are intended to promote consumer protection but, without careful consideration on scope and impact, are likely to instead create complexity and uncertainty.

Rather than prescribe specific measures that may be ill-suited to achieve the desired ends, an outcomes-based approach to requirements (such as those outlined in Articles 9 through 17) is more likely to deliver on the AI Act’s goals. This approach would begin by clearly articulating the outcomes needed to promote EU values of fairness and non-discrimination in the context of high-risk AI systems. Such an approach would give regulated actors the flexibility to adopt the measures or mitigations best suited to achieving the enumerated goals within the context of the specific technology, scenario, and deployment at issue. It would also spur further development of measurement and mitigation techniques, and the preparation of harmonized standards or common specifications that can be tailored for specific scenarios.

The AI Act calls in Article 41 for the Commission to adopt “common specifications” through implementing acts where harmonized standards do not exist or are insufficient. It is vital that the EC not show a preference for standards that advantage EU-based companies, and we strongly urge the Commission to ensure that any AI-related specifications used in regulations or conformity assessment procedures do not create unnecessary obstacles to trade. The EC should use international standards as a basis for regulation, or if not, be prepared to provide scientific or technical evidence to explain why it has deviated from an international standards. In addition, the EC should treat conformity assessment bodies located in the U.S. as favorably as it treats those on its own territory.

Disclosure of source code to market surveillance authorities, as required in Article 64, could seriously put at risk important trade secrets and IP rights, and contravenes established best

practices for digital trade at international level. Furthermore, we do not believe the source code of an AI system would be necessary for market surveillance activities.

The enforcement structure of the proposed AI Act is a complicated system with each Member State designating national competent authorities and a national supervisory authority. This complex structure requires each Member State to build expertise sufficient to understand and regulate state of the art technologies. This creates difficult burdens on each Member State, and any country that fails to bring in sufficient capacity will face difficulty in effectively regulating. In the end, this may discourage investments in lower risk technologies because of uncertain regulatory processes and outcomes. Instead, regulation would be more effective and better support innovation when it is developed by regulators with deep subject matter expertise.