Response of Microsoft Corporation to the European Commission's Inception Impact Assessment on Artificial Intelligence Legislation

(10 September 2020)

Microsoft appreciates the opportunity to respond to the European Commission's Inception Impact Assessment ("IIA") on its proposal for a legal act setting out requirements for artificial intelligence ("AI"). We support the Commission's goal of ensuring that AI evolves in a manner that respects EU values and fundamental rights. An appropriate regulatory framework for AI could advance the responsible development and use of AI both within the EU and internationally. Given the EU's deep integration into the global economy, any legislative framework for AI also should be interoperable to the greatest extent possible with efforts in other jurisdictions and forums to promote trustworthy AI.

In our response to the Commission's February 2020 AI White Paper ("AI White Paper Response," uploaded separately), we welcomed the Commission's proposal to adopt an incremental, risk-based approach to AI regulation. We noted that such an approach—one that imposes mandatory requirements on a discrete and clearly defined set of high-risk AI scenarios—will help protect people and society against AI use cases that raise significant risks of harm, while giving Europe's AI sector the flexibility it needs to grow and mature.

We continue to support that approach. Given the many nuances raised by the various scenarios in which AI can be deployed, we believe the Commission can most effectively achieve its goals through a mix of binding requirements for scenarios that pose the greatest risk, combined with soft-law approaches (e.g., codes of conduct, self-regulatory mechanisms) for lower-risk scenarios that incentivize the use of governance mechanisms and tools for promoting trustworthy AI. Microsoft addresses these issues primarily from the perspective of a developer and supplier of AI solutions that customers across the public and private sectors use for an almost unlimited range of purposes. These various uses may raise very different risks. In light of this reality, we urge the Commission give careful thought to which obligations are most appropriately placed on developers of multi-purpose AI solutions, and which are most appropriately placed on deployers.

Microsoft supports Option #4 of the IIA—namely, a combination of Options 1 through 3 that considers the different levels and types of risks that different AI scenarios may raise. This combination of measures is vital to ensure that the EU's overall regulatory approach to AI is meaningful, balanced, and effective. It bears repeating at the outset that there is no "one-size-fits-all" approach to AI regulation. Many AI systems pose low or even no risks to individuals or society (*e.g.,* AI systems that optimize storage of items in a warehouse or fix typing errors); these systems do not require new or mandatory regulation. And where meaningful risks do exist, they will often be different and context-specific, and thus require different mitigation measures, including regulation.

Here are our views on the Options:

Option #1: EU "soft law" (non-legislative) approach to facilitate and spur industry-led intervention (no EU legislative instrument).

Microsoft believes that industry has responsibility to develop and deploy AI that is trustworthy. We are investing heavily in AI governance standards and tools to put our ethical principles into practice across our engineering and sales teams and to help ensure that they guide our actions on a consistent basis.

Based on this experience, we believe developers and deployers of AI applications should adopt appropriate governance standards and procedures to support efforts to operationalize trustworthy AI across their organizations, and to use technologies, tools, and systems to help them identify and mitigate relevant risks of all types and levels. This standard could include, for example, the following requirements:

- Envision the full range of harms that any new AI system might impose on individuals and society both at the outset and throughout the product development lifecycle, and take appropriate mitigation steps;
- Provide appropriate training for those involved in the design, development, testing, and marketing of the AI system, and to assign specific individuals or groups within the company with responsibility for overseeing implementation and compliance;
- Adopt transparency obligations with customers, users, and other affected stakeholders to inform them about risks inherent in the use of the relevant AI system as well as the systems capabilities and limitations; and
- Adopt an escalation process through which employees and others can raise concerns and seek guidance on the company's compliance with its policies.

Deployers might have similar governance obligations, including for example a requirement to take necessary steps to avoid deployments of the AI system that could pose certain risks of harm. In many cases, these steps may be specific to the particular use scenario and/or sector at issue (we discuss these points further in our AI White Paper response). Similarly, public authorities should be encouraged to develop guidance on how best to achieve responsible governance when AI is used.

By leveraging private-sector-led efforts and related domain-specific expertise, the Commission's soft-law options could lead to the development of industry- or sector-specific codes of conduct that effectively target the unique risks that arise in specific scenarios and sectors (e.g., education, health care, autonomous transportation). As these codes mature, they could also foster convergence on common principles and best practices applicable to other areas as well.

This said, and while we continue to believe that such private-sector-led efforts must play a central role in promoting trustworthy AI and that the Commission should encourage the adoption of such efforts through various soft-law approaches, we also believe that these approaches alone will not always be sufficient to address the unique risks to fundamental rights and safety that might arise in certain scenarios (as we describe in more detail below). Thus, we do not believe that the "no EU legislative instrument" approach of Option #1 by itself would be appropriate.

- **Option #2: EU legislative instrument setting up a voluntary labelling scheme.**

Similar to our view on the soft law approach of Option #1, we see value in co-regulatory efforts to promote trustworthy AI, which might include efforts such as the voluntary labelling scheme described in Option #2. A co-regulatory approach may be particularly appropriate in cases where regulatory frameworks exist that require interpretation or adaptation in the light of AI, as well as in cases where AI usage could cause risk, but that risk does not rise to the level of "high risk." Option #2, therefore, should leverage existing laws and regulatory frameworks to the largest possible extent.

As noted in our AI White Paper response, labelling could prove beneficial for deployers when comparing and choosing among competing AI solutions or those affected by the development of an AI system. Such a scheme could signal to the market that a given AI system meets a defined set of requirements, such as the implementation of an organizational AI standard designed to ensure risk is identified and mitigated. That said, we think certain AI scenarios may raise such uniquely high risks that they merit the imposition of mandatory requirements. Thus, while we believe that a co-regulatory approach could be a useful component of a broader AI regulatory strategy, we do not think that Option #2 on its own would be sufficient to address all risks posed by AI in all scenarios.

To the extent a version of Option #2 is included in the final legislative package, we would encourage the Commission to consider a broader range of co-regulatory mechanisms beyond just labelling. Companies operating in the EU have significant experience in helping develop, and complying with, industry codes of conduct, formal and informal standards, and related self-certification schemes. Some of these mechanisms involve labeling, others do not. Developers and deployers of AI should be encouraged to leverage that experience in developing similar voluntary compliance mechanisms to promote trustworthy AI.

Any such mechanism might include objectives such being transparent about the limitations of a given system or the key data elements used to train the system, or adopting internal processes to promote accountability. It should also allow for regular, transparent, and independent monitoring and evaluation. One source of inspiration for relevant objectives could be the Assessment List for Trustworthy AI developed by the High Level Expert Group on AI (although not all the components will be either appropriate or necessary for all AI scenarios, given the many different settings in which AI can be used). We would also suggest drawing from the experience of companies that are already implementing trustworthy AI governance models.

Experience has shown that both self- and co-regulatory instruments, implemented in accordance with the different legal traditions of the Member States, can play an important role in delivering a high level of protection (for instance, under the Audiovisual Media Services Directive, and more recently under the General Data Protection Regulation). Measures aimed at achieving general public-interest objectives in AI applications are more effective if they are taken with the active support of the developers and deployers themselves. Building on voluntary measures, the proposed legislative package could include several co- or self-regulatory mechanisms tailored to specific scenarios and use cases, modelled on the Principles for Better Self- and Co-regulation, while creating a legislative backstop if industry fails to meet the objectives.

- **Option #3: EU legislative instrument establishing mandatory requirements for all or certain types of AI applications (see sub-options below).**

Microsoft agrees that certain AI deployment scenarios may raise such unique and significant risks that their use should be subject to mandatory requirements. Accordingly, we believe that Option #3 should be part of the Commission's legislative package (along with soft law options, for the reasons set out above). Given the almost infinite scenarios and domains in which AI can be deployed, it will be important for the mandatory elements of the legislative package to be carefully targeted at those AI deployments that raise the greatest risk of harm, and where existing EU and Member State laws do not already provide sufficient protections.

On this point, Option #3 of the IIA sets out three sub-options for the scope of any mandatory regulatory requirements—namely, that they should apply to:

(1) "a specific category of AI applications only, notably remote biometric identification systems (e.g. facial recognition)";

(2) "high-risk" applications as that term was defined in the AI White Paper; or

(3) all AI applications.

Given the nascent nature of AI development and deployment, Microsoft believes that, within this Option, the Commission should look to sub-options 1 and 2. One benefit to a focus on specific categories of AI applications (such as remote biometric identification) is that learnings from addressing these categories could inform future efforts to regulate other high-risk AI scenarios. Candidates for such future regulation could include AI applications that raise a meaningful risk of physical harm, such as AI-driven vehicles. We also believe that the legislative framework should include a mechanism that enables the EU, through new legislative instruments that build on the framework, to extend appropriate mandatory requirements into new areas based on the learnings generated from self or co-regulatory regimes, or from the enforcement of existing laws or new laws applying to specific systems. Because the harms will necessarily differ across different use cases, any future regulation must be tailored to the unique risks raised by the AI scenario at issue.

With regard to sub-option 1, Microsoft has been outspoken on the need to legislate FRT when used by public authorities, also in Europe despite the EU's comprehensive legislation on data protection. The use of FRT by public-sector authorities for remote identification, for example in public spaces, is widely recognized to raise unique and potentially serious risks to fundamental rights and other vital interests. We believe the Commission could significantly advance the discussion on trustworthy AI both within and outside of the EU by adopting a comprehensive legislative framework on such uses.

Within Europe, some Member States have begun to consider what an appropriate regulatory framework for police use of FRT might include. Courts are also beginning to define the permissible scope of use of FRT by public authorities. UK courts, for example, recently held that police use of FRT for remote identification must be authorized by law and subject to robust safeguards, in a case involving the South Wales Police. Regulation in this area by individual Member States could be usefully harmonized through EU-wide quality standards, such as on testing and transparency requirements, robust necessity and proportionality standards, and strong safeguards for the protection of fundamental rights.

Lawmakers in jurisdictions outside of Europe are similarly beginning to recognize the need for legislation in this space. The State of Washington in the United States, for example, recently adopted a law that regulates all public-sector uses of AI. Many of the requirements set out in the law effectively impose requirements not only public sector entities, but also on the *suppliers* of these AI technologies. Microsoft supported the Washington State legislation, which includes a number of important safeguards.

An EU-level legislative instrument could provide the legal basis necessary for police use of FRT, on the condition that such use is strictly necessary and proportionate, and subject to specific safeguards. These safeguards might include, for example, requirements that use of FRT for remote identification is allowed only in relation to most serious crimes or imminent risks to life, and in specific locations for limited times; that police may not use FRT to monitor individuals in the exercise of their fundamental rights (e.g., participating in a demonstration); that police develop robust data use and management policies, and conduct impact assessments, before any deployments; that systems are deployed in open and transparent ways; and that humans be responsible for any decisions made on the basis of FRT. EU legislation could also impose obligations on developers of FRT intended for such uses, such as requirements to make available an application programming interface (API) or other technical capability to enable legitimate, independent and reasonable testing for unfair bias.

- **Option # 4: combination of any of the options above taking into account the different levels of risk that could be generated by a particular AI application.**

As indicated above, Microsoft supports Option #4—specifically, a combination of Option #1 (soft-law measures), Option #2 (a voluntary labelling scheme or similar approaches), and Option #3 with sub-options 1/2 (mandatory requirements, including for public-sector use of FRT in public spaces). To ensure that the Commission's legislative package can adequately address the many different contexts in which AI can be deployed, and the very different levels and types of risks that these scenarios may pose, we believe that this combination of options is both appropriate and necessary – dependent on the risk level.

* * * * *

Once again, Microsoft welcomes this opportunity to respond to the Commission's IIA. Any questions about this response should be directed to Cornelia Kutterer, Senior Director European Government Affairs (cokutter@microsoft.com).