Meta's AI Act Position

Meta is in favour of regulation that is risk-based and technology neutral. This approach regulates the uses of the technology, rather than the technology itself. As a result, said approach ensures that the regulation is applied proportionately, introducing requirements to ensure protections in high-stakes settings, whilst avoiding hindering innovation in lower-risk areas. The original draft of the AI Act is, for the most part, underpinned by these characteristics, which we welcome.

The following principles would help to ensure that the final text retains that same focus, avoids duplication of other regulations, and is responsive to recent and future developments in AI technology.

Principle 1: The AI Act should maintain the risk-based approach and not create an additional regime for foundation models (Art. 28b - 4 Column Document 379d)

Recommended Approach: Maintain the technology-neutral, risk-based approach of the AI Act.

Foundation models are not inherently risky. As with other AI systems, the risks arise dependent on the context in which they are deployed. It is unnecessary, therefore, to introduce requirements for providers of foundation models. Our recommendation is to retain the risk-based, technology-neutral approach of the EU AI Act and reject these additions.

Compromise position 1: Providers who make their foundation models available through open source or similarly permissive licences that:

- **(i) provide open access to models;**
- **(ii) further the goal of fostering collaboration and innovation; and**
- **(iii) permit downstream users to use, reproduce, distribute, copy, create derivative works of, and make modifications to the foundation model**

should be exempt from requirements for providers of foundation models.

The AI Act should incentivise approaches that support the EU's goals for fostering AI innovation in Europe. In its Parliament version the AI Act includes an exemption for open source AI systems, in recognition of the critical role that open source development plays in driving innovation and delivering economic benefits from new technologies. In the coming years, access to foundation models will play a similarly crucial role in driving AI research, development, innovation and adoption. It is essential, therefore, that the AI Act facilitates widespread access to, and innovation in foundation models.

To do so, providers of foundation models should be granted an exemption from the requirements of the Act whenever they decide to make their models available under open source or similarly permissive licences. An approach of this type, which can be described as *open innovation,* would not only allow European researchers, developers, and citizens to benefit from advances in

foundation models, but also contribute to the creation of higher-performing, safer, and more secure foundation models as a broad community is able to test, scrutinise and improve openly available models.

Please note that Principle #2 below applies independently and regardless of the current compromise.

Compromise position 2: Providers of foundation models should be subjected to a tailored obligation regime.
If the decision is made to introduce some requirements for all foundation models, by virtue of their nature alone, **a distinction of such requirements must be made between providers**

- **who make their models available** in an open and transparent way, such as **under open source or similarly permissive licences that:**
    (i) provide open access to models;
    (ii) further the goal of fostering collaboration and innovation; and
    (iii) permit downstream users to use, reproduce, distribute, copy, create derivative works of, and make modifications to the foundation model.
- **and those that take a closed approach**.

In addition, improvements must be made to the current text to ensure that requirements are technically feasible and tailored to their purpose. Requirements applicable to all foundation models might focus on transparency, data governance, technical documentation, and risk assessment, in line with industry best practices, while providers of closed models may be expected to meet additional requirements, so as to provide additional assurance and oversight of those models. These additional measures need not apply to open models, as these models are at the disposal of more downstream developers, who can in turn scrutinise the software, identify and fix potential issues and therefore improve performance, safety, and security.

In this regard, we recommend a tiered regime in which Art.28b applies only when the foundation model is released under a closed system. If the foundation model is released under open source or similarly permissive licences, on the other hand, we propose a new Art. 28c to be included in the AI Act, amending Parliament's proposed 28b to better adapt to the nature of open models and to continue to maintain that risk-based approach that is core to the Act.

Please note that Principle #2 below applies independently and regardless of the current compromise.

Principle 2: The AI Act is not the right place to regulate copyright, which is addressed by existing EU regulations. (Art. 28b, paragraph 4b and c – 4 Column Document 379d)

Regardless of the treatment of foundation models, it must be clarified that copyright provisions (in this case, Art. 28b, paragraphs 4b and 4c) should not be addressed in the AI Act. The rules

introduced in the AI Act should build upon existing legislation, not duplicate it or clash with it. The matter of copyright obligations is already covered by Directive (EU) 2019/790 of the European Parliament and of the Council. The AI Act should, thus, defer to it. 4b and 4c should be removed from the text. In particular:

- **28b(4)(b):** The requirement to provide safeguards against the generation of content in breach of Union law is vague, overbroad, and at odds with fundamental EU principles of proportionality and legal certainty. Ensuring that adequate safeguards are in place should be the responsibility of the user of the generative product, since they are the ones that are most familiar with the functionality of the system, the audience it is used by, and its functionalities.
- **28b(4)(c):** As the EU Directive on Copyright in the DSM (articles 3 and 4) already provides control to rights holders over the use of their protected works for the purposes of training AI, the focus should be to encourage and facilitate industry collaboration e.g. for the development of workable standards to ensure the effective control of rights. The proposal concerning copyright law in Art. 28b(4) does not go to the specified objectives of the AI Act. It is broad and unworkable, and, moreover, there is already an extensive and robust EU legal framework in place ensuring IP protection.

Principle 3: The AI Act should avoid duplicating existing and planned EU regulations.

As the AI Act has progressed, its scope has expanded beyond the risk-based, technology-neutral proposal put forward by the Commission. In some cases, this has resulted in provisions which are duplicative of other EU laws. This will lead to confusion and potential conflict of regulatory requirements.

Specifically, the European Parliament has proposed amendments to add new types of systems to Annex III, which are already regulated in other regulatory instruments. These include:

- **AI systems intended to be used for influencing the outcome of an election or the voting behavior (Annex III paragraph 8, point aa - 4 Column Document 837a):** Given that back-end systems are excluded, it appears as though this amendment is aimed at systems, or their outputs, that natural persons would be exposed to. This could include political advertising, non-political content relating to elections such as 'get out and vote!' campaigns, or content relating to causes such as climate change, social justice, or reproductive rights that are not party political, but which often feature in political discourse and can shape voting behaviour.
  The Digital Services Act (DSA), which is a content regulation and which includes the specific obligation for Very Large Online Platforms (VLOPs) to manage systemic risks relating to "any actual or foreseeable negative effects on civic discourse and electoral processes" is the appropriate instrument for addressing content concerns. The AI Act should not duplicate that regulation.

- **Recommender systems used by VLOPs under the DSA (Annex III, paragraph 8, point ab - 4 Column Document 837b):** AI systems intended to be used by social media platforms that have been designated as very large online platforms (VLOPs) under the Digital Services Act (DSA). Similarly, Annex III(8)(ab) targets recommender systems, which are already regulated in the DSA and do not require separate measures.
    - First of all, the original list of Annex III includes areas such as law enforcement, employment, education, asylum, critical infrastructure and access to public services. Social media recommender systems are not operated in these potentially sensitive areas, where the effect could be of legal nature or similarly significant.
    - Secondly, under the DSA, providers of Recommender Systems are subjected to a wide range of obligations, mostly around transparency, risk assessment and mitigation. When drafting AI regulation, regulators should build upon existing legislation that already impacts AI, without creating tension with existing obligations.

Similarly, The Parliament's text proposes labeling AI generated content as a solution to combat the risk of misinformation from AI generated deep fakes.

- **Labeling (Art. 52, paragraph 3- 4 Column Document 515):** An emerging concern relates to the risk of misinformation from AI generated deep fakes. The Parliament's text proposes labeling this type of content as a solution. However, it is not clear that labeling is the best approach to address this risk. AI technologies are evolving rapidly, with new techniques and products emerging all the time. Rather than being prescriptive about how companies should address emerging concerns, the AI Act must be flexible enough to allow for evolving best practices to be adopted, as emerging risks become better understood, and standards are established. This could be further explored in the Code of Conduct on Disinformation and/or via peer collaboration and standard-setting bodies. For example, this could be done by developing a framework that enables users to distinguish audio or visual content generated by AI that would otherwise be indistinguishable from reality. Moreover, the DSA already places a requirement under Article 35 for platforms to mitigate risks in this area, and it's important that the AI act does not create conflicting or duplicative requirements.