Bloomberg L.P. annex to the European Commission consultation on the White Paper on Artificial Intelligence

Bloomberg welcomes the opportunity to provide comments on the European Commission's consultation on the White Paper on Artificial Intelligence. Please find below more detailed answers to the open questions in the consultation. We would be happy to discuss further any of the points we have raised in our response if the Commission would find that useful.

Section 1 - An ecosystem of excellence.

Question: Are there other actions that should be considered?

In all of these efforts, it will be very important to set appropriate and realistic metrics and goals. The goal of democratizing access to AI technology is a laudable one, but a number of milestones would need to be achieved to move the needle. Focusing the efforts of the research community and partnership with the private sector are crucial for determining what is actually possible, or is just about to become possible. Notably, quantum computing, which is mentioned in the consultation document, is still very much a research problem (many such problems, in actuality), and appropriate goal setting in scientific research is fundamentally different from encouraging uptake of more mature technology.

Conversely, we should be aware that the field is evolving rapidly, and the range of capabilities and constraints is changing quite literally on a weekly basis. Whatever regulatory frameworks, guidelines or initiatives are put in place will therefore need to be able to be adapted at a very rapid pace, or risk being leapfrogged and made less relevant by technology. Notable examples of the technological evolution of this kind are the development of generative adversarial neural networks, enabling e.g. style transfer in video to produce extremely realistic fake video content, and adversarial machine learning more generally, allowing black box attacks against a wide range of machine learning systems.

Lastly, we cannot afford critical advances in AI to be treated as a substance of competitive advantage by private enterprises and kept from the public. Strong incentives ought to be in place for open access research and reproducibility of said research, to avoid concentration of resources in walled gardens.

Section 2 - An ecosystem of trust

Question - Do you have any other concerns about AI that are not mentioned above? Please specify:

The realistic capabilities of AI should be well understood and socialized, to avoid use of AI in applications where simpler methods will suffice. AI systems are fundamentally data driven, and we currently lack rigorous engineering practice to reason about the design, operation and failure modes of machines that contain (potentially rapidly changing) data as critical parts of their operation. Fundamentally, a data-driven AI pipeline is a much more complex system than a "traditional" software system. Whereas model checking, correctness proofs and other tools to certify traditional software systems exist, applying them to machine learning and AI systems is still an area of research. Note, for example, the issues surrounding adversarial examples (which we now know are unavoidable for certain classes of AI systems) as an illustrative case study.

Question - Do you think that the concerns expressed above can be addressed by applicable EU legislation? If not, do you think that there should be specific new rules for AI systems?

Other

Other, please specify:

The legislation in question must be carefully thought through to consider future developments (see previous comments) and not to stifle innovation, or, conversely, to avoid creating misaligned incentives. For example, General Data Protection Regulation and similar regulations imply, among other things, that personally identifiable information can only be used for the purpose it was collected. That may indeed be appropriate in context of passive collection of personal data (e.g., by mobile apps manufactured by private enterprises). But, scientific innovation provides many examples of discoveries and progress that arise in an unanticipated fashion. Data sharing is well recognized as crucial for transparent, reproducible research. Thus, data collected for one purpose may later be used for a novel purpose previously unavailable due to lack of technological capability. There ought to be mechanisms, perhaps similar to reuse authorization for clinical trial data, allowing data reuse subject to review and anonymization within an appropriate mathematical framework (e.g., differential privacy). But, to work within such a framework is currently a challenge, due to sophistication of the methods involved. Thus, an actor in the market may be incentivized to advertise a purpose that is overly broad to cover many possible future use cases, unless the tools and know-how are widely available.