techUK welcomes the opportunity to provide feedback on the Commission’s proposed Artificial Intelligence Act (AIA). It will take time to fully unpack the implications of this legislative proposal and it will come down to the final wording of the bill’s articles to determine what will and won’t fall in scope, but it will undeniably have significant ramifications for the development of AI powered applications in Europe and broader consequences for the entire global AI industry. Below is an overview of our initial feedback on the current AI legislative proposal:

AI definition

The definition of ‘AI system’ is very broad and goes beyond what would normally be considered as ‘intelligent’. It also appears to include statistical processes and software or indeed any computer system more generally, even when their use is not within the context of techniques which are traditionally understood to be AI. Such a broad definition increases the number of technologies that fall in scope of this regulation. It would be helpful to have a clearer and potentially narrower definition. In the UK, the ICO has opted for a more targeted definition, focusing on supervised, unsupervised, and reinforcement learning[1].

Classification of high-risk AI systems

The rules for the classification of high-risk AI systems as included in Article 6 and Annex III is overly broad and would encompass AI applications that are not intended to be covered by the Regulation. For a more proportionate and effective application of the law, the Regulation should recognise that for an AI system to be considered high-risk, there should be the high probability that it would cause harm to the user. In addition, the Act also fails to recognise key contextual elements which would determine whether an AI system is high risk or not. Specifically, whether the AI is playing an advisory role or whether it directly makes a decision. Advisory systems, even in ‘high-risk’ areas should not be high-risk.

In addition, the AIA needs to recognise that for most of the applications considered “high-risk” there are already existing laws and regulations which will apply (i.e. health & safety, IP rights, manufacturing standards, liability, etc.) and ensure that any AI requirements that may be introduced do not contradict or duplicate these provisions. This would create legal uncertainty that is likely to impact AI innovators, particularly SMEs.

Further consideration is needed as to whether some of these concerns can be addressed by other means, for example greater use of transparency/explainability. Equally, it’s important that the sector is provided with enough encouragement to come up with new technologies and new ways of working which might address some of these concerns.

Members would also like clarity on whether non-high risk AI systems who voluntarily fulfil the same requirements as high-risk AI systems will similarly receive a CE marking.

Remote biometric identification vs. biometric authentication

The scope of high-risk biometric identification is currently not clear enough. Whilst the February 2020 AI White Paper makes a rightful distinction between remote biometric identification and biometric authentication, the recent Commission proposal on AI fails to do so. We agree with both of the definitions in the White Paper with the former defined as practices where the “identities of multiple persons are established with the help of biometric identifiers at a distance, in a public space and in a continuous or ongoing manner by checking them against data stored in a database”, while

[1] AI definitions, Information Commissioner’s Office (ICO)

the latter is defined as "a security process that relies on the unique biological characteristics of an individual to verify they are who they say they are". techUK urge the European Parliament and the Council of the EU to explicitly clarify this distinction between biometric identification and biometric authentication. This is the correct approach, as it ensures that uses of facial recognition with implications for fundamental rights are restricted, while applications that merely compare the one-to-one likeness of a person to a document should not be subject to the same requirements. This distinction is also recognised by the Council of Europe in their feasibility study, where they note that such use of AI does not carry the same impact on human rights as other uses of AI. While we welcome the consistency in substance across the different institutions, the use of terminology between the European Commission White Paper and the Council of Europe study is inconsistent. While the Commission refers to biometric authentication as a security process, the Council of Europe refers to the same practice as remote biometric identification.

To avoid the risk of confusion as well as different interpretations by regulators and stakeholders, terminology in the framework must be consistent and preserve clear distinctions between different applications of facial recognition technologies. While we recognise that identity verification datasets can be used to populate databases which are then used for other facial recognition purposes, the use of individual's data in identity verification more broadly is not intended to impact them directly. The new framework should make clear the definitions of the different use cases of facial recognition, namely identification, authentication, and verification. This difference in use cases is also already reflected in Article 9 of the EU General Data Protection Regulation (GDPR) with only biometric data processed "for the purpose of uniquely identifying a natural person" considered a special category of personal data.

Legal uncertainty

The current legislative proposal has reserved powers for the Commission to add to the list of high-risk applications in the future. This creates legal uncertainty and makes it difficult for companies' compliance planning. There is also a general concern that the investment required to ensure compliance with the proposal would not only drive up the cost of AI solutions on the market but also the compliance costs for users. This includes the governance processes and infrastructure to run the risk management process, in addition to ensuring that an organisation has qualified and trained teams to carry out the conformity assessment.

Conformity assessments for high-risk applications

The ex-ante conformity assessment associated with high-risk AI applications would place a considerable strain on businesses, especially start-ups and innovators by adding massive friction to the AI development cycle. A combination of ex-ante and ex-post may be purposeful as long as ex-ante mechanisms are limited to self-assessment only. It is also important to consider how these mechanisms would apply across different sectors that are already regulated.

More balanced responsibilities for AI providers and users

The European Commission's proposal includes a series of obligations to be met by AI providers before placing AI systems on the market (Article 16). This split in responsibilities between AI providers and users does not look adequate, especially considering the realities of the market roll-out of AI solutions. Software providers supplying customers with Machine Learning tools cannot control how their customers use these tools and deploy their own models. They also cannot be held responsible for how the AI systems are used. They also have no control of or access to their customers' datasets and have no clarity on how the AI models are being trained.

To address this, we believe that the co-legislators should thus reassess the responsibilities and roles of providers and users to better reflect the reality of designing an AI system, compared to operating it. Ultimately, the AI Act should offer flexibility to allocate responsibilities to the actors that can most appropriately ensure compliance, notably by ensuring the freedom of the parties to allocate responsibilities through contractual obligations.

The EU's approach must also take adequate account of the long and complex supply chains for AI products and services. It's important that we find a way of ensuring that the company which puts the final AI product on the market has trust in the components which have gone into the product.

techUK would welcome a simplified explanation of the concerned parties and how they interact. Members have mapped out how they believe various parties such as the Provider, Notifying Body, Notified Bodies, National Competent Authority, etc. will interact, but this is complex. Although relationships between users and providers should be left to commercial contracts, it would be helpful to see a diagram depicting how the Commission envisages these different parties working together.

Finally, in order to determine responsibility in the supply chain for carrying out the risk-assessment, it would be helpful to have a clearer guidance on what constitutes a 'substantial modification' in Recital 66.

Areas of further clarification

We support the proposal's attempt at a risk-based approach, recognising that certain applications or contexts will not pose risks to fundamental rights and freedoms. Although there are a number of areas where we would welcome further clarity. For example, Article 5(1) (a), there is a lack of clarity on which systems and uses could potentially be in scope, with no apparent link to the risk management process for High-Risk use cases. It would therefore be helpful to provide a clear definition of what is meant by "*Subliminal techniques beyond a person's consciousness in order to materially distort behaviour*" and secondly, guidance on what legal standard or process would be used to determine and enforce this provision, particularly in relation to demonstration of *'psychological harm'*. For these prohibited AI applications further clarity is needed on how this will be applied in practice. For example, how will this apply to existing applications such as a social media recommendation system, if an algorithm was to recommend extremist content?

Article 10(3) requires that "training, validation and testing data sets shall be relevant, representative, free of errors and complete." Although we do not disagree with the spirit of the requirement, it demands a level of perfection that is not technically feasible. This requirement must reflect feasible, best practice standards and be capable of adaptation - for example the requirements relating for datasets used in a medical context and/or relying on biometric data will be quite different to those used to automate routine form completion or improve a retail function. The risk is that all AI producers will be in violation of the requirement. The Regulation could include some form of qualification that would maintain the spirit of the requirement ("Providers shall make reasonable efforts to ensure that training, validation and testing data are relevant", etc…), while being implementable in practice. Alternatively, techUK believes a better approach would be to allow industry to continue to develop data standards, such as via data labelling which would provide users of AI systems with an understanding of the quality and qualities of the training data. techUK believes industry is best placed to develop these technical standards.

Under Article 14 (Human Oversight), we would challenge the reference to "full understanding" of the capacities and limitations of AI systems, as this is simply a requirement that cannot be complied with. On the other hand, we agree that humans should have a role in detecting issues and providing feedback on high-risk AI models when anomalies occur.

Further guidance on Article 64 (2) would be helpful, particularly in relation to the definition of "source code". This could be the code of the trained AI model, of the validated AI model, or the code to build the AI model. The code may not always be retained so guidance on retention period would be helpful. In some cases, the code may also be confidential or constitute commercially sensitive information. It may be worth considering other options to satisfy the objectives of the provision, including metrics to measure how certain fields influence the output of the model and therefore determine the level of risk. Requesting access to source code also increases risk exposure for ML processes from a cybersecurity perspective and could lead to supply chain and compliance risks for companies.

Recital 16 states that the prohibition on unacceptable uses would not be stifling for research however there is no other mention of research in the regulation when it comes to high-risk AI systems for instance. AI research is crucial for innovation and its essential that the AIA does not inadvertently disincentivize investment in AI research. techUK would therefore welcome a more general statement on research 'as it relates to all AI systems' not being stifled by the regulation.

Working towards global AI standards

Regulating AI should be done in a way that prevents unnecessary barriers to trade and investments. The EU should maintain an open dialogue with like-minded countries such as the US and UK in order to ensure that a similar approach to AI is taken based on shared democratic values and that European citizens are able to benefit from global innovations.

Sandboxes

techUK strongly supports the AI Act's provisions for building voluntary regulatory sandboxes for the development, testing and validation of innovative AI systems. However, we believe that the current proposal is not ambitious enough and may lead to potential fragmentation in their implementation and operation. Going forward, sandboxing should be made a cornerstone of the proposal to encourage innovation.

Next steps

As the legislative process now moves over to the European Parliament, we call on legislators to work together with industry and like-minded international partners, to find solutions to some of our common AI challenges and strike a balance between regulation and innovation that ultimately promotes trust in and drives forward the adoption of ethical and responsible AI.