ITI Promoting Innovation Worldwide

10 September 2020

Requirements for Artificial Intelligence

ITI views on the European Commission Inception Impact Assessment

The Information Technology Industry Council (ITI) welcomes the publication of the Inception Impact Assessment (IIA) on Requirements for Artificial Intelligence, and appreciates the opportunity to provide comments building on our contribution to the February 2020 White Paper on Artificial Intelligence.

As the premier advocate and thought leader for the global technology industry, ITI and its members share the firm belief that building trust in the era of digital transformation is essential. At the same time, it is important to promote innovation to ensure Europe's global competitiveness and security. For this reason, we welcome the IIA's goal to foster the development and uptake of safe and lawful AI that respects fundamental rights and ensures inclusive societal outcomes, all while preserving an enabling environment for innovation.

We firmly believe that AI can bring about significant benefits to our society. AI-driven medical diagnostics can alert doctors to early warning signs to help them treat patients more capably. Increasingly intelligent systems are able to monitor large volumes of financial transactions to identify fraud more efficiently. Small and medium-sized enterprises (SMEs) can gather new insights and improve their businesses by using AI and data analytics made available to them through online services.

Therefore, it is crucial for Europe to not only look at the potential harms of using AI, but also consider the potential economic and social harms of limiting the use of AI, which may decrease its positive impact on our communities. Technological innovations bring innumerable benefits to the European economy and society. We are already experiencing the benefits of AI in an array of fields. Promoting these advances is no less important than managing any potential challenges.

We thus urge the Commission to take into consideration the wide array of possible applications of AI technology, and their different use cases and risk factors when approaching the development of policies related to AI. We believe that, through a context-specific and risk-based approach, policymakers can develop a framework that adequately addresses any unintended risks that AI may pose while simultaneously promoting technological innovation.

Problem definition

1. Fundamental rights

While we are aware of the potential risks that may arise from some applications of AI, we believe that context is key in identifying appropriate policies to mitigate this risk. The IIA mentions for instance issues related to fundamental rights and inclusion. The technology industry recognises the need to mitigate bias, inequity, and other potential harms in automated decision-making systems. We share the goal of **responsible AI adoption and development**. As technology evolves, we take seriously our responsibility as enablers of a world with AI, including through seeking solutions to address potential risks.

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

Our industry is committed to partnering with relevant stakeholders to develop a reasonable, effective, and balanced accountability framework that takes into account the different actors and phases of developing and deploying AI systems. As leaders in the AI field, ITI members recognise their important role in making sure technology is built and applied for the benefit of everyone. **Approaches must be context- and risk-specific** and should consider that not all AI applications affect individuals' fundamental rights. Such AI applications would not require an all-encompassing fundamental rights-based approach and may not warrant any additional regulatory intervention.

In fact, many AI uses have little or no impact on individuals' rights, such as in the context of industrial automation and the use of analytics to streamline automobile manufacturing, to improve baggage handling and tracking at busy European airports. This is also true for consumer products, where machine learning can support users to optimise a device's battery usage or reduce wait time linked customer service or technical support. AI development should not be disrupted with new stringent obligations that could significantly slow the adoption of AI and hamper innovation.

Moreover, where fundamental rights are affected, AI applications used in specific sectors (e.g. healthcare, financial services, transportation) are already subject to sectoral regulation that is often geared towards addressing risks to fundamental rights of individuals (e.g. Medical Device Regulation (EU) 2017/745, Payment Services Directive (EU) 2015/2366). In addition, the Commission is currently contemplating relevant updates or revisions of existing legislation, including initiatives noted by the IIA. While it is important to assess if existing, domain-specific EU regulations are exhaustive, it is also important to further underline that they already cover many of the most common concerns, including by providing sufficient assurances regarding the safety of connected and AI-embedded devices. Any future regulatory activities should therefore be limited to address discrete and specific issues not covered by existing rules.

When considering new rules tackling AI's impact on fundamental rights, the European Commission should not seek to duplicate the existing regulatory framework – GDPR in particular. It should also consider whether market access-related conformity assessment approaches are appropriate to ensure the enforcement of fundamental rights. First, impacts to fundamental rights are more likely to arise during the technology's deployment or usage, rather than at manufacturing stage. Secondly, imposing such pre-market assessment on standalone software, which are easy to distribute, should be carefully assessed in terms of proportionality so as to not limit innovation. Thirdly, this kind of regulatory approach requires clear ways of measuring and demonstrating compliance, such as the availability and use of relevant technical standards, the availability of testing protocols to test implementations against those standards, and, even if uses on a voluntary basis, notified body with the technical experience and bandwidth.

We also take note of the specific concern that the IIA puts forward on surveillance by biometric facial recognition. Our industry takes this issue seriously and recognises our important role in making sure AI technologies, like facial recognition technology, are built and applied in a way that benefits everyone. It is critical that society, governments, and the technology sector work together to begin to solve some of the most complex issues, including this one. New regulations and policies should be compatible with existing rules like GDPR to protect users without causing harm or unintended consequences.

2. Product Safety

The IIA mentions product safety as one of the potential areas of focus for a potential forthcoming legislative initiative on AI. We recognise and share the crucial aim of the European Commission of

ensuring that all goods marketed in the EU, whether or not governed by sector-specific legislation, are safe and effective. As alluded to above and in the IIA, the EU is leading several discussions on how to ensure product safety while taking into account new technologies, including through the review exercises of the General Product Safety Directive (GPSD) and Product Liability Directive (PLD), as well as sector-specific initiatives including the revision of the Machinery Directive (MD) and updates to the Radio Equipment Directive (RED). Each of these potential legislative processes bear significant implications for the manner in which technology firms across a wide spectrum of business models market safe and effective products and services in the EU. As the Commission contemplates potential further regulatory action governing AI alongside these initiatives, we invite policymakers to see all of these exercises and existing laws in connection with each other to ensure a coherent approach that promotes new technologies while managing any potential challenges. Considering these efforts in parallel will help understand what, if any, gaps remain, and how to best resolve any remaining challenges. In addition, such coordination will prevent the inadvertent development of any technical barriers to trade, which might limit access to productivity-enhancing ICT goods and services.

As a principle, should the Commission choose to take further action in this field on the basis of the results of the present IIA, we believe that such action should be technology neutral, meaning that the technology itself is not regulated but rather that the law sets forth more general pillars that can remain fit for purpose for future innovations regardless of the technology in question. Given that AI is a rapidly evolving technology, regulation which targets AI as such would likely become obsolete and possibly disproportionate as the technology, our understanding of the underlying science, and use cases evolve. This is also why we caution against the introduction of new product safety requirements specifically targeting AI. We encourage the European Commission to focus on specific applications of the technology, outcomes, and governance approaches for the use of AI technology, instead of regulating the technology itself, which will allow for flexibility.

As we have pointed out in the context of the review of the GPSD, stand-alone software typically does not pose the same type of heightened safety risks associated with traditional physical products. As the IIA notes, with limited exceptions, liability and product-specific legislation does not provide for the regulation of stand-alone software, and it is unclear that assurance mechanisms associated with such legislation – such as testing requirements – would be proportionate or fit-to-purpose in this context. We therefore urge the Commission to carefully consider whether legislative tools aimed at ensuring product safety are necessary or appropriate when assessing any potentially relevant risks associated with stand-alone software.

3. Liability

AI presents great opportunities for society in different fields yet raises valid concerns around responsible and safe deployment. We believe that the clarification of rules around liability, currently designed for physical products, is an appropriate area of focus. There are also important considerations about finding the appropriate balance of ex-ante, preventive rules, and ex-post measures, including remedies. We support an effective and balanced liability regime that fosters trust in the use of AI, provides a clear path for redress and adequately compensates victims for damages, while allowing for incremental improvements and innovations that come with placing AI systems on the market.

In many cases the existing liability framework will be easily applied in an AI context and we suggest that the EU maintain a strong presumption against altering it except in response to significant and demonstrable shortcomings. Should a need for future legislative or administrative action be identified in areas that involve increased risks for end-users of AI applications, it should be addressed in a sector-specific manner, with new regulation or suggested legislation addressing clearly identified issues,

based on evidence and data, and designed to avoid overreach. Sector-specific safe harbour frameworks or liability caps are also worth considering in domains where there is a concern that liability laws may otherwise discourage socially beneficial innovation. Updating such sector-specific regulation, rather than adopting sweeping changes to general product liability frameworks, would allow for more precise targeting of remedies for identified gaps in liability coverage.

If the existing liability regime falls short of addressing new challenges arising from specific applications, legislative intervention should be limited to filling in the gaps or addressing clear shortcomings, while avoiding an overhaul of the existing framework, which has proven to provide an adequate balance in protecting consumers while encouraging the launch of innovative products in the market. It is also important that due consideration is given to the diversity of the actors in the supply chain, to avoid that liability is disproportionally spread to actors that could not reasonably be expected to bear responsibility for situations beyond their control.

We also consider that the business/individual can fulfil the requirements of the Product Liability Directive (PLD) and recover damages if a product containing AI technologies causes harm to a business or individual. In this sense, **amendments to the PLD to cover embedded AI are unnecessary, since the directive is technology-neutral** and strikes the right balance between the obligations of consumers and producers, thereby creating legal certainty. Still, it is crucial to recognise that there is a fundamental difference between on the one hand a hypothetical, undefined risk, and on the other the danger based on the product's fault or its use in a specific context. Strict liability frameworks like the one set up by the Product Liability Directive (PLD) remove any consideration of intent or negligence. Therefore, strict liability should only apply for high-risk AI applications defined as sector, use case, complexity of the AI system, probability of worst-case occurrence, irreversibility and scope of harm in worst case scenarios. Further comments on this definition are further down in this paper in the section about high-risk AI applications (pages 8,9). Manufacturers should instead be equipped with a right to cure or correct identified violations with consumers directly. This would also be in the interest of fostering consumer trust in AI applications.

Policy options

We believe that in order to avoid overregulation, any potential future initiative targeting AI will need a clear, targeted scope focusing on those high-risk AI applications where issues are most likely to arise.

Since there is no single widely agreed-upon definition of AI, it will be important for policymakers to provide greater clarity if they plan to seek specific rules for AI functions. An essential factor is to properly identify AI and its different categories, including the component parts of AI systems beyond algorithms, as well as to define related key terms such as machine learning. Some algorithms have been applied for decades but do not constitute "Artificial Intelligence" or "machine learning" systems. The first task is to determine what is AI and what is not. There is a difference between the latest wave of AI systems that learn from data and experience, and traditional software and control systems that operate according to predictable rules, which have long been embedded in a wide variety of high-risk systems from flight control to pacemakers to industrial settings. As mentioned above, we believe that the risks associated with traditional software and control systems that make probability predictions are already adequately addressed by existing regulation.

We caution the Commission about considering to significantly expand the scope of possible future AI regulation to the open-ended category of "automated decision making." This would go against the initial, thoughtful direction proposed in the AI White Paper that proposes to focus on the risk-based, double-criterion for sectorial and application/use-based AI technologies. If AI were defined as "automated decision making" for the purpose of possible future AI regulation, it would create

disproportional, unjustified regulatory obligations that would not only deter development and deployment of AI-based applications in Europe, but also automated systems that do not pose any significant risk of harm.

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

Standardisation is a necessary tool to bridge any potential AI regulations and practical implementation. The EU should support global, voluntary, industry-led standardisation, and safeguard the work and processes of bodies developing international standards. Global AI standards reflect broad consensus around technical aspects, and work is currently underway on standards to address management, and governance of the technology. Building on decades of experience and lessons learned, technical standards development is underway to help frame concepts and recommended practices to establish trustworthiness of AI inclusive of privacy, cybersecurity, safety, reliability, and interoperability. Standards and their use in regulations must not be done in a manner that creates market access barriers or preferential treatment; rather, they should work for the benefit of the international community and be applicable without prejudice to cultural norms and without imposing the culture of any one nation in evaluating the outcomes/use of AI.

Beyond the support of international standards development, the Commission should use its approach to AI as a way to incorporate greater flexibility into its approach to standardisation, thus recognising the value of standardisation for new technology and enabling regulators alike to draw upon the broadest range of fit-to-purpose solutions in determining the most appropriate global, industry-driven, voluntary standards. A greater degree of flexibility with respect to the standards that may be used to demonstrate compliance with relevant AI-specific requirements would yield positive outcomes for both domestic and global innovation, consumer protections, and market openness.

Option 2: EU legislative instrument setting up a voluntary labelling scheme

In general, voluntary labelling schemes can play a role in promoting consumer trust, if they are well designed, recognised and sufficiently specific. It remains unclear how this could play a role for AI powered services and products, given the limited amount of information provided in the IIA. Indeed, its usefulness would very much depend on the scope of the products considered, their applications, and who the end-user is. A very general voluntary label may have limited impact, be misleading or could even lead to adverse outcomes if poorly designed. The use of AI may not be immediately obvious or important to the user. Some products may involve very different AI-powered features, which may be hard to reflect on a single label, while multiple labels will impact the user experience and lead to label fatigue, desensitizing the user to the intended message. It is also unclear whether the label will be product specific or could apply to an entire entity.

Similarly, voluntary labelling would also require extensive both pre-labelling assessment and post market surveillance schemes, which raises questions linked to proportionality. Voluntary labeling should therefore be considered in specific contexts, focusing on areas where its user trust has been a proven deterrent to adoption.

In conclusion, given that AI systems themselves do not constitute a physical product or service, we have questions about how such labelling could be applied in a manner that achieves the objective of facilitating information to consumers. Broadly speaking, any voluntary labelling approach should not become a de-facto market entry requirement for AI products and services in Europe. Further, technical challenges around electronic labelling (e-labelling) would need to be broadly addressed for products

and services that do not have a physical shape on which to affix a label; therefore, flexibility should be considered in those scenarios. As a general matter, we strongly encourage the Commission to adopt international best practices for e-labelling in allowing the display of regulatory and other required information via electronic means. Additionally, voluntary labels should be based on international standards and recognised by all EU Member States.

Option 3: EU legislative instrument establishing mandatory requirements for all or certain types of AI applications

The IIA mentions that, under option 3, an EU legislative framework would "establish certain mandatory requirements on issues such as training data, record-keeping about datasets and algorithms, information to be provided, robustness and accuracy and human oversight." (page 5) Before commenting on the sub-options proposed by the IIA, we would like to provide additional comments on these aspects, as we believe setting mandatory legal requirements may in some cases hinder the development of beneficial AI applications. In general, the potential burden linked to these requirements calls for a risk-based approach to regulatory requirements.

- *Training data*

We fully acknowledge the importance of robust training data sets in the development and deployment of AI. However, rather than focusing on the data sets themselves, which often will reflect biases that exist in the real world, we suggest focusing on testing outcomes of the AI systems before deployment or applying safeguards against biased outcomes after deployment. Stereotypes can be perpetuated either in recommendations, searches, or quality of tool so considered quality-control and review processes should be in place and outputs tested to protect against this. This requires testing and human involvement in the development of AI with diverse teams that are continually evaluating in the development and innovation of AI.

Some AI models may require less strict requirements to data sets if they are designed with the appropriate caveats and caution – requirements should be set in connection to the purpose and what is required to ensure non-discrimination in relation to that purpose. We see an urgent need for the Commission to clarify how training data requirements will interact with GDPR (including the right to be forgotten and data minimisation) and clarify the requirements addressed to the party that is best positioned to perform the quality control of the data. We also urge the concept of 'sufficiently representative' to be defined more clearly.

- *Keeping of records and data*

We caution against the introduction of mandatory record-keeping requirements for datasets used to test, train, or operate AI systems on an ongoing basis. If keeping of data could lead to revealing details of AI systems or underlying code, this could risk undermining privacy, copyright, and trade secrets, infringe on IP rights, and heighten cybersecurity risks, privacy, and data manipulation risks. Instead, we urge the Commission to assume an approach that looks at outcomes rather than process, and which is compatible with the GDPR's data minimisation principle.

Moreover, keeping vast amounts of data would be unworkable for many companies given how AI is developed in a constantly iterative way.

Lastly, it is important to note that there are no common widely-used data naming conventions, no formatting standards or concurrent versioning systems used for data, with efforts to address these

currently underway; these factors would further complicate mandatory sharing requirements in this field.

- *Information provision*

We believe that Transparency does not automatically equate to better control or decisions of AI systems. For example, the driver of a car does not need to fully understand the systems in a vehicle to be able to drive the vehicle safely. Similarly, users of AI would in most cases not need to have a detailed understanding of the workings of the technology to use it responsibly. In any case, GDPR already provides for a general obligation of transparency including an obligation to inform the individual about their rights and enable them to contest their decision and even seek redress.

Transparency, in our view, is best achieved through ensuring understandability and interpretability. **Understandability** should allow users of AI to understand broadly how an AI application works and how their data is being used to create a better user experience for them individually. Rather than introducing obligations to disclose technical features, we recommend an approach in which understandability is prioritised to build consumer trust. **Interpretability** on the other hand is geared towards allowing technical experts to understand the rationale behind an AI's decision/outcome. Both aspects are important, and we encourage policymakers to think of transparency in these terms to make explicit the objective of any potential transparency requirements.

We further urge that there should be a differentiation for transparency requirements for AI in high-risk applications being used in consumer-facing v. B2B products and services. For B2B scenarios, we do not see reason to share such information unless the information in question is deemed to be critical for public interests including safety. This is because excessive sharing obligations might risk IP rights and contractual arrangements between business partners. Further, an organization that develops AI cannot proactively monitor the way its customers are using AI.

As a general principle, if AI is playing a substantive role within a high-risk AI application, that fact should be easily discoverable along with some insight into the nature of the role AI is playing by those who have a legitimate interest.

Public disclosure will typically be appropriate for applications designed for or affecting consumers in areas of public interest (e.g. government services or healthcare). However, public information about B2B use of AI should not be required except in case of clear public interest.

- *Robustness and accuracy*

A safety-by-design approach should be implemented for all high-risk AI applications. Internal documentation and monitoring will be key for companies developing high-risk AI applications to assure their customers of the product's quality and security. Mandating additional, far-reaching reporting or documentation requirements in addition to existing legislation such as, for example, the General Product Safety Directive (GPSD) would be premature and could hinder industry from finding best-suited solutions to challenging, complex processes. Due consideration should be given to already existing laws so as not to create a rigid system that could risk longer term safety of products and accuracy of AI systems if innovation is not incentivised.

- *Human Oversight*

We need to be mindful of different AI application areas and to what extent humans need to be involved throughout the lifecycle of an AI application. For example, it is useful to have a human

monitor an automated decision in an air traffic control tower and override decisions made by the AI if necessary (for example in an emergency). In such a case, the AI de facto replaces the human and therefore, human oversight is needed continuously. However, for other, less critical situations, we may not require detailed human involvement e.g. for handling baggage at an airport.

Individual use cases and the risk of adverse outcomes associated with an application should determine the degree of involvement of humans in reviewing machine-generated decisions. In some cases, human oversight can not only lead to delays, in others, accuracy of outputs or even human safety could even be undermined by human interventions (for example for mathematical calculations).

3a. Sub-option 1 – Regulating Biometric Surveillance

As already mentioned above, our industry takes the issue of biometric surveillance seriously and recognises our important role in making sure AI technologies, like facial recognition technology, are built and applied in a way that benefits everyone. It is critical that society, governments, and the technology sector work together to begin to solve some of the most complex issues, including this one. Possible new regulations and policies should be compatible with existing rules like GDPR to protect users without causing harm or unintended consequences.

3b. Sub option 2 – Regulation limited to High-Risk AI applications

Our industry welcomes the IIA's intention to lay out a differentiated, risk-based approach with a distinction between high- and low-risk AI applications, based on a number of criteria. However, as we had previously pointed out in our comments to the Commission's White Paper on AI, it is important that the Commission carefully considers its definition of high-risk AI applications. The use of "sectors", for instance, may lead to a too broad categorisation. We thus encourage developing a categorisation that takes into account sector, use case, complexity of the AI system, probability of worst-case occurrence, irreversibility and scope of harm in worst case scenarios e.g. individual v. larger groups of people, and other criteria. Those criteria should be clearly defined to ensure legal certainty for AI developers and be translated into high-level principles that could be transformed into operational requirements set up in the form of industry-led standards, certification schemes or codes of conduct.

More specifically, we urge policymakers to consider the following specifications for high-risk AI applications in order to build on the White Paper's differentiation also mentioned in the IIA, and ensure for the development of principles-based rules:

- **Specify what constitutes high-risk AI applications based on probability and irreversibility**: To ensure proportionality, the definition should be augmented to better reflect well-established interpretations of risk as a function of severity and likelihood. For example, high-risk could be defined as AI systems that either (a) may cause catastrophic irreversible harm and there is a possibility that such harm may occasionally occur, and (b) may cause serious harm and such harm is probable. More clearly reflecting a nuanced understanding of high-risk within the framework would make clear that the objective of the framework is to mitigate harm for (a) and reduce the likelihood for (b).

- **Acknowledge and define AI's opportunity costs**: In several instances, using automated systems can greatly reduce risk. In air traffic control, using an automated tool paired with human oversight is an example of how AI can reduce risk as opposed to a situation in which air traffic controllers could make mistakes due to fatigue or distraction - factors that do not affect a machine. Analysis about the spread of pandemics is another example where limiting

the use of AI is likely to lead to potentially bigger risks than possible negative consequences of the AI system being deployed for this purpose.

- **Remove "exceptional instances" clause**: We support the notion of clear and predictable cumulative criteria, as well as clarity over what constitutes a high-risk use of AI, and ideally the negative impact or concrete consequences that can reasonably be expected on affected parties. However, the "exceptional instances" clause in the AI White Paper, which the IIA also refers to, is too open-ended and should be removed to avoid legal uncertainty. For example, the notion that applications affecting consumer rights could potentially fall in the high-risk category seem overbroad, unjustified and against the objective of focusing only on well-defined areas of risk. In addition, the instances to which the White Paper appears to refer seems to be appropriately covered by existing legislation (non-discrimination provisions in labour law and consumer laws).

- **Align references to damages with the PLD**: The 1985 Product Liability Directive (PLD) empowers European consumers to receive compensation for damage caused by defective products. The PLD applies to any product sold in the European Economic Area with a 3-year limit for the recovery of damages. The PLD defines damage as death, personal injury, or damage to the product in questions or other products of a consumer. This definition could be a good basis to support the definition of what constitutes high-risk AI. We would advise avoiding references to immaterial damages that could potentially lead to waves of compensation claims for producers on illegitimate grounds and lead to a backlog in assessing cases all while mostly being covered already by existing legislation in the fields of data protection, non-discrimination and freedom of expression.

3c. Sub-option 3 – Regulation Covering all AI Applications

Given the variety of applications that benefit or may benefit from AI, context is key in identifying appropriate regulatory options. As we have noted, not all AI applications pose the same level of, or any, risk to safety or fundamental rights and not all potential harms are new or related to AI only. For instance, many AI uses have little or no impact on individuals' rights, such as in the context of industrial automation and the use of analytics to streamline automobile manufacturing, to improve baggage handling and tracking at busy European airports. This is also true for consumer products, where machine learning can support users with optimize a device's battery usage, or reduce wait time linked customer service or technical support. Finally, in business-to-business contexts the same AI application can be used in different ways by the customers which increases the need for a context-specific assessment of each use case to determine the risk incurred.

Moreover, as mentioned above, we believe that many AI applications are already covered by existing legislation in the field of fundamental rights, data protection, product safety and liability. Potential new legislation should only be considered in instances where regulatory gaps are identified that cannot be addressed through self- or co-regulatory approaches. Completing a revision of the current EU legislative framework is the first crucial step to have a holistic and comprehensive overview on the identified legislative gaps in order to address them through additional guidance or concrete amendments of existing EU legislation

We strongly caution against considering a one-size fits all regulatory approach. It would in fact risk disrupting AI development with new stringent obligations that could slow down the adoption of AI and hamper innovation to the detriment of consumers and businesses in Europe alike, particularly if the Commission chooses to regulate AI technology itself instead of focusing on the governance

approaches or use cases. This approach would thus ultimately run counter to this IIA's very objective of promoting the development and uptake of AI in Europe.

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 detailed above, we would welcome a context-specific and risk-based approach. We believe that regulatory measures should target those high-risk AI applications for which specific regulatory gaps have been identified, while avoiding overly precautionary approaches that may stifle innovation. Moreover, legislative approaches should be flexible enough to account for the rapidly changing and fast-paced technological advancement in this sector.

As mentioned above, context is key in identifying appropriate measures concerning AI. Many uses – e.g. in medicine, financial services, or transport – are already subject to sectoral regulation. In many instances, the essential requirements already contained in harmonized legislation may be sufficient in covering risks presented by applications of AI.

A proper assessment of applicable laws should precede new legislation, with a view toward evaluating whether new rules are actually needed, avoiding conflicts of law, and ensuring that both existing and forthcoming regulatory requirements prioritize international compatibility and reliance on global, industry-driven, voluntary, consensus-based standards. In cases where regulatory shortcomings are identified, adapting existing laws would be the appropriate way forward.

Enforcement mechanisms

As mentioned in our response to the White Paper, we believe that a combination of ex-ante risk self-assessment and ex-post enforcement for high risk AI applications would be the most appropriate enforcement mechanism for any future regulatory scenario. This solution would likely achieve intended results within much faster timeframes and without hampering innovation or creating unnecessary burdens. For instance, requiring companies to carry out and document risk assessments would be analogous to the data protection impact assessment under GDPR. Such an approach would also build on existing industry practices, including the ethical, legal, and due diligence practices that guide the responsible and trustworthy development of AI. To clarify compliance and facilitate accountability, regulators should assess what actors are best to act at what stage in the AI lifecycle. For example, the developer of AI is responsible for conceptualising and training the AI, whereas deployers have the best visibility of the use case for the AI.

This solution would address the many concerns that an ex-ante regulatory approach would pose. For instance, the existing conformity assessment infrastructure may lack resources or expertise to effectively and efficiently carry out testing of AI. In addition, we are concerned that stringent ex-ante requirements may create problems for products already in the market, R&D of early stages products and software updates throughout a product's lifecycle.

Conclusion

To sum up, we believe that there cannot be a "one-size-fits-all" solution to properly address all the issues related to Artificial Intelligence. In this sense, a mix of solutions as proposed by Option 4 of this IIA seems to be the most balanced approach. However, we urge the Commission to consider our recommendations when developing its approach. We see great value in the EU encouraging and promoting industry-led initiatives as proposed in Option 1 of the IIA. We believe that industry can solve many issues related to technical aspects, management, and governance of AI technology, as well

as frame concepts and recommended practices to develop trustworthy AI applications that consider privacy, cybersecurity, safety, reliability, and interoperability through processes of voluntary, global and industry-led standardisation. When it comes to regulation, we believe that new legislation should be considered only where legislative gaps are clearly identified. For this reason, we caution against horizontal regulatory solutions, as proposed in Sub-option 3c, which would result in overly stringent requirements and ultimately slow down the adoption of AI and possibly hinder innovation. At the same time, we welcome the consideration of risk as the key factor in defining the scope as proposed by Sub-options 3a and 3b. However, we urge the Commission to carefully consider the definition of high-risk considering use case, complexity of the AI system, probability of worst-case occurrence, irreversibility, scope of harm in worst case scenario and sector.

***