POSITION PAPER WITH EU TRILOGUE RECOMMENDATIONS

Towards a balanced and future-proof AI Act

July 2023

The Computer & Communications Industry Association (CCIA Europe) welcomes the progress made on the Artificial Intelligence (AI) Act by the EU Council and the European Parliament. While the EU co-legislators have made useful improvements to the initial text, certain issues still need to be addressed during the interinstitutional "trilogue" negotiations. To that end, this position paper sets out CCIA Europe's recommendations for delivering an AI Act that promotes trust and innovation in AI in their true sense.

I. Maintain a risk-based approach to AI regulation

In order to let AI innovation thrive, while addressing potential risks in parallel, the AI Act should set clearly defined rules based on risk. Only a technology-neutral approach, applying the most stringent requirements to truly high-risk applications, can achieve this objective.

Recommendations:

1. Keep the focus on high-risk use of GPAI and foundation models
2. Maintain exemption for GPAI & foundation model providers prohibiting high-risk use
3. Apply balanced and implementable rules to GPAI and foundation models
4. Avoid unnecessary copyright requirements
5. Streamline the allocation of responsibilities along the value chain
6. Agree a fair and workable implementation timeline for AI systems in scope

II. Avoid unnecessary red tape and regulatory overlap

Enhancing legal certainty for developers and deployers of AI systems is crucial, so particular attention should be paid to avoiding unnecessary red tape and regulatory overlap. Indeed, the duplication of legal requirements should be prevented at all costs to reduce complexity.

Recommendations:

7. Keep Article 6's focus limited to truly high-risk AI applications
8. Steer clear of duplicating existing legal requirements (e.g. DSA, political ads, DMA)
9. Find the right balance on task allocation in Annex III
10. Ensure consistency between the EU's financial framework and creditworthiness evaluation

III. Prevent unintended consequences

In order to avoid unintended consequences, a clear and limited list of prohibited AI systems needs to be designed. The introduction of export bans in the AI Act would go beyond the scope of its legal basis and could undermine the EU's international trade commitments.

Recommendations:

11. Avoid unintentionally banning legitimate practices
12. Refrain from including export bans in the AI Act

Introduction

The Computer & Communications Industry Association (CCIA Europe) welcomes the progress made on the Artificial Intelligence (AI) Act by the EU Council and the European Parliament. While the EU co-legislators have made useful improvements to the initial text, certain issues still need to be addressed during the interinstitutional "trilogue" negotiations.

To that end, this position paper sets out CCIA Europe's 12 recommendations to streamline the negotiations and achieve the AI Act's dual objective of promoting trust and innovation in AI. The paper's three overarching themes, highlight the need to:

I. Maintain a risk-based approach to AI regulation
II. Avoid unnecessary red tape and regulatory overlap
III. Prevent unintended consequences

The EU has the opportunity to create the first horizontal regulation on AI in the world. Yet, it also needs to ensure that clearly defined risks are effectively addressed while leaving enough flexibility for European developers to continue to innovate in useful AI systems.

I. Maintain a risk-based approach to AI regulation

In order to let AI innovation thrive, while addressing potential risks in parallel, the AI Act should set clearly defined rules based on risk. Only a technology-neutral approach, applying the most stringent requirements to truly high-risk applications, can achieve this objective.

1. Keep the focus on high-risk use of GPAI and foundation models

CCIA Europe is a long-standing advocate of a risk-based approach to regulating AI. Like any other technology, AI systems can be used for very positive purposes, but also in negative ways. The initial AI Act proposal therefore rightly focuses on high-risk use cases of AI systems, and not on specific technologies underpinning AI as such.

While both the European Parliament and the EU Council departed from this original approach presented by the European Commission, the positions of the two co-legislators are also very different and leave enough room for the creation of a balanced framework that addresses the different concerns at stake.

We believe that the EU Council's position on general-purpose AI (GPAI) systems is closer to the AI Act's original risk-based approach, as it focuses on the high-risk uses of such systems. However, Articles 4b and 4c of the Council General Approach are broadly formulated and would need to be further adjusted to avoid that all GPAI systems are being targeted, which would also impact many useful and low-risk systems. For example, GPAI also includes simple models that are able to recognise straight lines and other basic shapes, which have many useful industrial, educational, and similar applications.

The EU Council approach rightly acknowledges that the AI Act's high-risk requirements are not best suited for either general-purpose AI systems or foundation models, and thus need to be further adapted by way of implementing acts. In order to avoid overburdening

developers of GPAI in the EU, the obligation to follow a conformity assessment procedure should be removed, in line with the Parliament text.

A useful and sensible approach would be to maintain the focus on high-risk uses of GPAI systems and foundation models when applying specific requirements, based on the Council text, while creating a list of proportionate obligations that are adapted to the specificities of such systems. This approach would subject GPAI systems or foundation models to a set of tailored obligations if they meet the criteria of Article 6 and are deployed in one or more of the high-risk areas of Annex III.

2. Maintain exemption for GPAI and foundation model providers prohibiting high-risk use

Article 4c of the EU Council's General Approach provides a useful exemption to the obligations applicable to GPAI providers, if the latter explicitly exclude, in good faith, all high-risk uses in the instructions of use or information accompanying their GPAI systems. This approach should be maintained and could be further extended to GPAI systems that are developed by providers for their own services only. Indeed, if a GPAI system is not open for use by third parties or downstream deployers, the provider of the system remains in full control of said GPAI system and potential risks remain very low.

Similarly, as the focus should remain on high-risk uses of AI or GPAI systems, low-risk systems should not be subject to any of the high-risk requirements, as this clearly would be disproportionate. Should, however, the GPAI system be substantially modified – i.e. in such a way that the system falls in one of the high-risk areas of Annex III and meets the requirements of Article 6 – it should be considered high-risk, as every other AI system.

This meaningful exemption should also apply to providers of foundation models who prohibit any high-risk uses in the instructions of use or information accompanying their systems, or only using such proprietary systems for their own services. Similarly, if the foundation model is substantially modified in such a manner that the model falls in one of the high-risk areas of Annex III and meets the requirements of Article 6, it should be considered high-risk.

3. Apply balanced and implementable rules to GPAI and foundation models

The EU Council rightly acknowledges in Article 4(b) that the high-risk requirements for AI systems are not well suited for GPAI systems and should therefore be adapted by way of implementing acts. CCIA Europe believes that high-risk requirements should not apply to GPAI systems, especially as regards the obligation to conduct a conformity assessment procedure.

In Article 28(2), the European Parliament strikes the right balance by only requiring providers of GPAI systems to provide deployers with the technical documentation and all other relevant and reasonably expected information capabilities, as well as technical access or other assistance based on the generally acknowledged state of the art that are required for the fulfilment of the obligations of the new provider. This approach is well suited to regulating these types of systems and helps to avoid unnecessary red tape.

Moreover, we strongly advise against the application of very stringent obligations to developers of foundation models, as proposed by the European Parliament. In particular, Article 28b of the Parliament position lists a number of requirements applicable to providers of foundation models that go far beyond the actual obligations for providers of high-risk AI systems. Think, for example, of the obligation to identify, reduce and mitigate reasonably foreseeable risks to the environment, democracy and the rule of law, in addition to the health, safety and fundamental rights of natural persons.

Other requirements introduced by the Parliament include new copyright requirements that are impossible to meet and put the careful balance struck by the EU Copyright Directive in peril. The obligation to involve independent experts to determine how to comply with the obligations of providers of foundation models is disproportionate and unworkable in practice.

The EU Council and Parliament should maintain the focus on applying balanced and implementable rules for GPAI or foundation model providers. Industry is hopeful that the co-legislators will find a meaningful way to reconcile their respective positions. CCIA Europe recommends to focus applicable requirements on high-risk uses only, as suggested by the EU Council, and to streamline responsibilities along the value chain, as proposed by the European Parliament, by requiring GPAI providers to only provide relevant technical documentation and assistance to downstream providers. Should the co-legislators decide to apply a specific layer of obligations to providers of foundation models, which we oppose, we underline that such obligations need to be proportionate and technically implementable.

4. Avoid unnecessary copyright requirements

CCIA Europe strongly advises against introducing new copyright requirements in the AI Act, as the European Parliament has proposed. The obligation for providers of foundation models that are used for the purpose of generative AI to document and make publicly available a summary of the use of training data protected under copyright law is unnecessary and simply unworkable in practice.

The EU's existing copyright framework, including the EU Copyright Directive that came into force only two years ago, is very comprehensive and already covers AI. The European Commission also recently reiterated that EU copyright rules apply to AI and dismissed the need to introduce additional rules in this field.

In fact, this whole new copyright debate revolves around data, which is crucial to train AI systems. They use data to learn and improve their performance, but also to adapt to new environments and to make accurate predictions. Training AI systems on diverse and representative data also helps to reduce potential biases. Today, many AI systems train on web-crawled data – i.e. the sources for the training of such systems are the entire open web. The transparency requirement proposed by Parliament is disproportionate, as it would amount to disclosing all the content on the internet and would be impossible to meet.

What is more, Article 4 of the Copyright Directive already grants rights holders the ability to allow or disallow the use of their works. This directive strikes a careful balance between the various interests at play and now has to be applied and enforced consistently. The directive also empowers rights holders to decide *ex ante* whether their content can be used or not.

The introduction of *ex post* requirements is therefore unnecessary and disproportionate. The AI Act protects fundamental rights and safety, it therefore is not the right legal instrument to address issues related to intellectual property and copyright.

Moreover, it must be underlined that such mandated data sharing would need to meet existing safeguards on the protection of personal data, but also intellectual property and trade secrets. Indeed, much of the data that would need to be disclosed under the proposed amendment may be proprietary to the provider and would amount to the disclosure of trade secrets.

That is why introducing specific copyright rules in the AI Act would go far beyond its scope and objectives, and risks significantly delaying the progress made on this crucial file. Fostering and streamlining industry collaboration for the development of state-of-the-art standards to ensure efficient rights management could be explored separately.

In line with our recommendations, we underline that compliance with the transparency and content safety requirements introduced by the European Parliament in Article 28b(4)(a) and (b) should rather rest on the deployers of generative AI than on providers. Because deployers at the application layer are best placed to understand the final use and context of such systems. For example, in the case of OpenAI's ChatGPT, it is indeed at the level of ChatGPT – or any other deployer using it – that the implementation of such requirements is most effective, and not at the level of the underlying GPT3 foundation model.

5. Streamline the allocation of responsibilities along the value chain

Both the EU Council and the European Parliament added provisions, in Article 23a(1)(e) and Article 28(1)(ba) respectively, to ensure that a deployer making substantial modifications to an AI or GPAI system that make it high-risk, becomes the new provider of the system and must meet the related requirements. We believe that this improves the allocation of responsibilities in the AI value chain and takes the realities of the AI ecosystem well into account.

CCIA Europe agrees that providers should offer a sufficient level of assistance to enable the new provider of the system to meet its obligations under the AI Act. Both the EU Council and the European Parliament oblige, in Article 4b(5) of the Council General Approach and Article 28(2) of the Parliament's position, providers of GPAI systems to provide the necessary information to other downstream providers, while ensuring that intellectual property rights and trade secrets are protected. The EU Council empowers the Commission to present implementing acts to ensure uniform conditions. We believe this approach should be maintained in the final AI Act.

The right allocation of responsibilities along the AI value chain is a crucial component of the AI Act. In order to fully account for the realities of this complex value chain, the AI Act's terminology needs to be adapted to reflect the number of relevant actors active throughout this chain. By differentiating between providers, deployers, and end users of AI systems, the European Parliament's report better reflects the reality and is, therefore, better suited.

In this complex value chain, it is important to place the AI Act's obligations on the party that is best suited to identify whether the use of a system can be considered high-risk or not, and to comply with the relevant requirements of the regulation – namely, the deployer

of such a system. As envisaged by the two co-legislators, the provider of an AI system should provide the necessary level of assistance to allow the deployer to comply with its obligations. The details of the necessary level of assistance should be defined, contractually where required, by the relevant parties. The publication of non-binding guidance from the European Commission could prove useful in this context.

6. Agree a fair and workable implementation timeline for AI systems in scope

The European Commission, EU Council, and Parliament all agree, in Article 83(2) of the AI Act, that the regulation shall not apply to high-risk AI systems other than large-scale IT systems that have been placed on the market, or put into service, before the date of application of the AI Act. This fair and proportionate provision further clarifies that it only applies if the AI systems at issue have not been subject to significant changes in their design or intended purpose, in which case they must comply with the AI Act's requirements.

This provision, which currently applies to high-risk AI systems, should be adapted to also include any other form of artificial intelligence in scope of the AI Act, depending on the final outcome of the negotiations between the co-legislators. Should GPAI or foundation models fall in the scope of the regulation, it must be clarified that the AI Act's requirements do not apply to systems placed on the market before the entry into application of the regulation, unless they are substantially modified. This is essential for companies, which need a high level of legal certainty to continue to invest and innovate in this field.

II. Avoid unnecessary red tape and regulatory overlap

Enhancing legal certainty for developers and deployers of AI systems is crucial, so particular attention should be paid to avoiding unnecessary red tape and regulatory overlap. Indeed, the duplication of legal requirements should be prevented at all costs to reduce complexity.

7. Keep Article 6's focus limited to truly high-risk AI applications

The EU Council and Parliament have made useful improvements to Article 6, which determines whether an AI system can be considered high-risk if it falls in one of the critical areas and use cases of Annex III. However, it must be underlined that a high level of legal certainty can only be achieved if the critical areas and use cases of Annex III are clearly defined and sufficiently targeted, allowing providers and deployers to assess whether their systems can be classified as high-risk.

Article 6(3) of the EU Council's general approach clarifies that AI systems whose output is purely accessory in respect of the relevant actions or decisions to be taken and are unlikely to lead to a significant risk to health, safety, or fundamental rights, cannot be considered high risk under the AI Act. The European Parliament proposes in Article 6(2) to classify AI systems as high-risk if they fall into one of the categories of Annex III and pose a significant risk of harm to the health, safety or fundamental rights of natural persons. In Article 3(1)(1b), the Parliament defines "significant risk" as "a risk that is significant as a result of the combination of its severity, intensity, probability of occurrence, and duration of its effects, and its ability to affect an individual, a plurality of persons or to affect a particular group of persons."

In addition, the Parliament mandates in Article 6(2) the European Commission to publish, after consulting the AI Office and relevant stakeholders, guidelines clearly specifying the circumstances in which the output of AI systems referred to in Annex III would pose such a significant risk of harm. CCIA Europe considers that the two approaches by the co-legislators are complementary and should be maintained in the AI Act in order to make sure it only targets truly high-risk AI systems. We underline that such an improvement to Article 6 can only be useful if the categories of Annex III are clearly defined and sufficiently targeted, if the definition of "significant risk" is maintained, and if clear guidelines on the concrete use cases are published by the Commission.

The proposed broadening of Annex III would considerably undermine any improvement to Article 6, and the lack of clear guidelines would leave companies with a high level of legal uncertainty. We invite the co-legislators to consider Article 6 and Annex III jointly, with a view to ensuring that a high level of legal certainty is effectively maintained.

CCIA Europe strongly opposes the European Parliament's introduction of a pre-notification mechanism in Article 6(3) of the report. We underline that the proposed mandatory notification process is inconsistent with the functioning of EU product safety rules, which require marketing authorisation procedures only in rare and extraordinary situations, and only for products posing exceptional risk, such as medicinal products. As it stands, this notification procedure would apply to a significant number of AI systems, without sufficient justification. It must be borne in mind that providers of AI systems already have a strong incentive, due to the risk of high penalties, to comply with the AI Act and to classify their AI systems as high-risk if the conditions are fulfilled.

Moreover, we are concerned that this notification process might overload National Supervisory Authorities and result in potential deadlocks. Companies willing to voluntarily notify their systems in order to benefit from the assessment of an authority and to ensure that they correctly classified their AI systems, should however be able to do so. Against this background, we recommend making the process purely voluntary.

8. Steer clear of duplicating existing legal requirements (e.g. DSA, political ads, DMA)

The European Parliament proposes, in point 8(ab) of Annex III, to classify recommender systems for user-generated content of very large online platforms (VLOPs) in the meaning of the Digital Services Act (DSA) as high-risk AI. We underline that recommender systems for user-generated content are merely used to provide users with a personalised experience with regard to the content they see. They do not present a significant risk to the health, safety, or fundamental rights of users per se, and should not be classified as high-risk AI. Overburdening companies with overlapping requirements risks slowing down the deployment of recommender systems, which are essential to the supply as well as the safety of these services. Such requirements would not only deprive consumers and businesses of the many benefits of recommender systems, they would also limit platforms' ability to ensure an age-appropropriate experience and to prevent malicious activity.

The list of VLOPs has only recently been published by the European Commission and the DSA still needs to enter into application before it can be effectively enforced. It is thus inappropriate to extend the list of obligations which VLOPs are subject to under the DSA to other obligations under new legislation, such as the AI Act. In addition, we underline that

the European Commission is the sole enforcer of the obligations of the DSA with regard to VLOPs and that the addition of new requirements in the AI Act risks conflicting with the enforcement structures of the two regulations.

Moreover, CCIA Europe strongly opposes the idea of introducing high-risk classification of AI systems based on the size of the provider. The size of a provider does not account for the risk that an AI system poses whatsoever – it is either high-risk, or it is not. Under the DSA, VLOPs already face the obligation to identify, analyse, assess, and mitigate risks that are systemic and stem from the use of their services in the EU, including recommender systems. The inclusion of VLOPs in the AI Act will add complexity and legal uncertainty for European companies of all sizes, as their main objective is to continue to innovate and grow in the EU. In light of the above, we urge the co-legislators to remove this provision and to focus on truly high-risk use cases in Annex III of the AI Act instead.

Similarly, the European Parliament's addition to Annex III(1)(8)(aa) of AI systems intended to be used for influencing the outcome of an election, a referendum, or the voting behaviour of persons, does not only overlap with the DSA, but also with the proposed EU regulation on political advertising that is currently being debated. Indeed, this regulation specifically intends to increase transparency and accountability in relation to political advertising. It will create a comprehensive framework for political advertising, and specifically targets recommender systems, advertising services, and the potential risks they pose in the context of elections. This framework is therefore much better suited to address those matters than the AI Act.

In addition, the DSA obliges VLOPs to periodically identify, analyse, assess, and mitigate any systemic risks posed by recommender systems, including "any actual or foreseeable negative effects on civic discourse and electoral processes". With regards to the above, and in order to avoid overlapping requirements, we recommend entirely deleting this point from the AI Act.

Finally, CCIA Europe expresses concerns regarding the inclusion by the European Parliament, in Article 51(1a)(b), of an unnecessary and disproportionate requirement for gatekeeper-designated companies under the Digital Markets Act (DMA) to register all high-risk AI systems that they deploy, before they even put them into service. This requirement runs counter to the objectives of the AI Act on the one hand, which is to regulate AI systems based on the risks they pose, and of the DMA on the other hand, which is to regulate a limited number of very specific core platform services.

This requirement is unjustified and disproportionate, as it would negatively impact innovative companies only because of their size. It must be underlined that not all services operated by gatekeepers are successful or have an important reach, and that the mere reach of a company cannot serve as the sole indicator to assess potential risks. Moreover, it is unclear why any system should be registered before being put into service. We oppose any such unjustified requirements. Against this background, we recommend to entirely remove this provision.

9. Find the right balance on task allocation in Annex III

While the co-legislators adopted very similar language for point 4(b) of Annex III, CCIA Europe believes that the wording of this critical area should be further improved to avoid

unintentionally impacting low-risk AI applications. The proposed high-risk classification of AI systems intended to be used for task allocation based on individual behaviour, personal traits or characteristics, as well as for monitoring and evaluating performance in work-related relationships, is too broad and encompasses many common, low-risk applications. For example, call centres can use AI to route incoming calls and assign them to the relevant worker, based on language capability or location. Similarly, railway companies can use the same system to schedule their staff based on their preferences, including location. As it stands, such low-risk and beneficial uses of AI would be unintendedly classified as high-risk.

Indeed, the focus on the term "behaviour" is extremely broad and misleading, as it can also capture benign, factual elements, such as a person's movement or location. For example, in the case of ride-hailing or delivery services location is a minimum, yet fundamental, input to be able to fulfil a consumer request for these services. Similar elements or inputs are essential for numerous other useful and legitimate commercial practices, including most importantly those commonly used to warrant the safety of workers and users. We, therefore, recommend to rather focus on the term "performance", which better addresses the actual risks that this provision seemingly aims to capture.

Separately, the upcoming Platform Work Directive (PWD), currently under legislative review, sets out specific obligations on the use of algorithms and AI, including of systems used for task allocation, which covers similar – if not the same – requirements for information, transparency, and human oversight. It is therefore important to ensure consistency and coherence between the AI Act, the PWD and the General Data Protection Regulation (GDPR) for such systems and reduce regulatory overlap to a minimum.

10. Ensure consistency between the EU's financial framework and creditworthiness evaluation

The European Parliament added a useful clarification to point 5(b) of Annex III, setting out that AI systems used for the purpose of detecting financial fraud are excluded from the high-risk areas. It is crucial that companies can use AI systems to detect such fraud in order to comply with their obligations under Union legislation and in particular the EU's financial framework.

CCIA Europe strongly recommends maintaining this useful clarification in the AI Act, allowing companies to meet their obligations under Union law.

III. Prevent unintended consequences

In order to avoid unintended consequences, a clear and limited list of prohibited AI systems needs to be designed. The introduction of export bans in the AI Act would go beyond the scope of its legal basis and could undermine the EU's international trade commitments.

11. Avoid unintentionally banning legitimate practices

CCIA Europe reiterates that any blanket ban on AI systems needs to be clearly targeted at truly unacceptable practices in order to avoid inadvertently banning legitimate practices.

The European Parliament has considerably broadened the list of banned practices in Article 5, which greatly increases the risk of unintended consequences. For example, in Article 5(d) the Parliament proposes to completely ban the use of real-time remote biometric identification systems in publicly accessible spaces. This broad ban, however, would prohibit many commonly used products that do not pose any significant risk of harm. Think, for example, of virtual assistants controlled by voice.

We understand that the main priority of the European Parliament is to ban AI systems that can be used for surveillance purposes. CCIA Europe, therefore, recommends limiting this prohibition to the systems used by public authorities, while explicitly excluding systems that require an interaction with the user and are not intended for surveillance, such as virtual voice assistants powered by AI.

Nonetheless, CCIA welcomes the clarifications of both the EU Council and the European Parliament, in Recital (8), that verification systems which merely compare the biometric data of an individual with their previously provided biometric identification, are excluded from the scope of this ban. The EU Council usefully clarifies that such systems, if used for the sole purpose of confirming that a specific person is the person they claim to be, as well as systems used to confirm the identity of a person for the sole purpose of having access to a service, a device, or premises, are out of the scope of the ban. These legitimate practices are low-risk and already very common today. Hence, we call on the EU co-legislators to maintain these clarifications in the final AI Act.

In Article 5(1)(ba), the Parliament introduced a ban on biometric categorisation systems that categorise people according to sensitive or protected attributes or characteristics, or based on the inference of those attributes or characteristics. While the objective behind this new provision seems to be to rule out the discriminatory categorisation of people, and is therefore commendable, this blanket ban risks missing its target and being counterproductive. Indeed, such systems have proven to be useful to infer the age of users in order to protect children online and to fight the dissemination of child sexual abuse material (CSAM). They can also be used to detect deep fakes, to enhance accessibility, or to mitigate bias in datasets.

In its current form, however, this blanket ban could prohibit many legitimate AI applications. The approach of the European Commission and EU Council, which instead addresses biometric categorisation as part of the AI Act's transparency requirements, is better suited to serve this goal. No matter what, any ban always needs to precisely target the specific, harmful use case that it seeks to prohibit. Other use cases simply should not be banned from the outset, instead of being subject either to the AI Act's transparency or high-risk requirements, depending on the risk they actually present.

The Parliament also introduced, in Article 5(1)(dc), a ban on emotion-recognition systems in the workplace, without elaborating on the actual specificities of the high-risk use case concerned. While Parliament's intention to protect workers is commendable of course, the broad wording of the prohibition could in fact have the opposite effect. Indeed, AI systems can be used to protect the health and safety of workers, users, and citizens.

For instance, AI-powered systems can identify when the driver of a car dozes off and activate an alarm to wake them and avoid an accident. Such lifesaving AI applications would be entirely prohibited, due to the broad wording the Parliament used to define

"emotion recognition". CCIA Europe recommends clarifying this provision to exclude AI deployed for the purpose of physical and non-physical safety. Alternatively, we recommend the co-legislators to narrow the provision to specific high-risk use cases and include those in the list of high-risk areas of Annex III.

Similarly, in point 1(1)(aa) of Annex III the European Parliament included AI systems that are intended to be used to make inferences about personal characteristics of individuals on the basis of biometrics or biometrics-based data, including emotion-recognition systems, with the exception of prohibited AI systems. This provision also risks affecting low-risk applications of such technology, for example in the context of personal well-being, user feedback, or media analysis. For low-risk use cases, the transparency requirements of Article 52 are much better suited than the AI Act's high-risk requirements, which would impose a disproportionate burden on developers and deployers.

12. Refrain from including export bans in the AI Act

The European Parliament introduced in Article 2(1)(ca) of its position an export ban on prohibited AI systems in the meaning of Article 5 of the AI Act. The provision would prohibit the placing on the market or putting into service of AI systems referred to in Article 5 outside the European Union, where the provider or distributor of such systems is located within the Union. This measure, which seeks to introduce extraterritorial application of the prohibited practices under Article 5, is all the more concerning as the list of prohibited practices was considerably broadened by the Parliament.

CCIA Europe fully agrees that limiting the availability and proliferation of harmful AI is laudable and necessary. Yet, a unilateral approach that relies on banning entire categories of use cases, without proper analysis or impact assessment, is unlikely to have the desired effect. Instead, it could prevent effective international coordination on shared priority areas in the field of AI, including machine-assisted healthcare and weather forecasting. Export controls should be addressed in horizontal, technology-neutral legislation, following extensive international coordination and in accordance with WTO rules. The AI Act's legal basis does not allow for the introduction of export bans and could undermine the EU's international trade commitments.

Conclusion

CCIA Europe calls on the EU co-legislators to adopt a risk-based AI Act that is balanced and future-proof. We wholeheartedly support the main objectives of this new regulatory framework – i.e. promoting trust and innovation in artificial intelligence to the benefit of all Europeans. At the same time, we want to underline that the best way for the EU to inspire other jurisdictions around the world, is by ensuring that its regulation enables, rather than inhibits, the development of useful AI applications. As we enter the final phase of the negotiations, we remain committed to work constructively with the European institutions, with a view to ensuring that innovation can flourish across the EU.

About CCIA Europe

The Computer & Communications Industry Association (CCIA) is an international, not-for-profit association representing a broad cross section of computer, communications, and internet industry firms.

As an advocate for a thriving European digital economy, CCIA Europe has been actively contributing to EU policy making since 2009. CCIA's Brussels-based team seeks to improve understanding of our industry and share the tech sector's collective expertise, with a view to fostering balanced and well-informed policy making in Europe.

For more information, visit: twitter.com/CCIAeurope or www.ccianet.org

For more information, please contact:

CCIA Europe's Head of Communications, Kasper Peters: kpeters@ccianet.org