Computer & Communications Industry Association
Tech Advocacy Since 1972

Position paper on the EU Artificial Intelligence Act
4 January, 2022

1. Introduction

CCIA Europe[1] shares the European Commission's objective of building a solid framework that is future-proof, creates legal certainty and encourages innovation and trust in this key technology.

While the Commission's proposal is a good starting point, this paper points out several issues which, from our perspective, deserve further clarification by EU policymakers.

2. Clarifying the definitions and the scope of the Regulation

The definition of "Artificial Intelligence System (AI)" given in the AI Act in Article 3.1 as well as the list of techniques in Annex I is **too broad and could encompass nearly all modern software systems, even if they do not perform functions associated with AI based on previous common definitions.**[2] For example, linear regression is a statistical model and it should not be considered AI.

As currently drafted, this broad definition, in conjunction with the vague categorisation of "high risk" AI, will overburden companies with compliance measures. The proposed Commission definition of an AI system creates the risk of unintentionally regulating all traditional technology, not just AI, and may result in significant barriers to growth and innovation. "AI system" is defined so broadly that it goes beyond what society typically considers to be AI, and could include every day software, spreadsheets, GPS, search tools, texting, calendar tools, etc., because they use "logic-based" or "knowledge-based" approaches in development, and can generate outputs that influence their environment. Subjecting such technology to the Act's requirements, including the high risk requirements, could create substantial barriers to access and use of technology in the EU. The key to defining AI lies in focusing on what it is about AI technology that is different from traditional software and ensuring that the definition provides technically clear guidance on what is being regulated versus what is not (e.g., models developed using data driven

[1] The Computer & Communication Industry Association (CCIA Europe) is a not-for-profit membership organization that represents the world s leading providers of technology products and services.
[2] A definition of AI: Main capabilities and scientific disciplines High-Level Expert Group on Artificial Intelligence, AI HLEG (2019)

machine learning approaches instead of calculators). As it stands, the current definition could ultimately hinder innovation and create legal uncertainty for market participants in the EU.

In this context, we believe that **further defining the concept of AI would contribute to legal clarity concerning what is being regulated, and how parties should comply.** Any definition of AI should be less focused on how the technology operates and more on who is impacted by the deployment of solutions that use AI technology and how. The aim is to avoid an overly broad scope of the Regulation and to ensure a stronger focus on AI-specific characteristics. Therefore, **we recommend a revised definition of AI based on the below definition proposed by the European Commission's own High-Level Expert Group on AI:**

"Artificial intelligence (AI) refers to systems designed by humans that, given a complex goal, act in the physical or digital world by perceiving their environment, interpreting the collected structured or unstructured data, reasoning on the knowledge derived from this data and deciding the best action(s) to take (according to predefined parameters) to achieve the given goal. AI systems can also be designed to learn to adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)".

Article 3.2 defines "***provider''*** of high-risk AI systems as "*a natural or legal person, public authority, agency or other body that develops an AI system or has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark''*. The process of developing an AI system is complex, involving research, testing, experimentation and validation. This does not mean that there is already a product in mind, however, the "*with a view to''* concept could encompass this process and fall into the scope of the Regulation. Researchers cannot anticipate all potential downstream uses of their research, and even if there is a product idea underpinning development, the final version will often differ substantially from its original vision.

Moreover, this research often results in work products like research papers or demos that are not in itself AI products, however, there is the doubt of what would happen if these research publications are considered as "*placing on the market''* or "*putting into service".*

This broad and unclear language risks causing interpretational issues for EU manufacturers. **European AI research and development activity could be discouraged given the risk of falling into the Regulation's scope and having to undergo a laborious conformity assessment.**

Article 3.14 defines a **"*safety component of a product or system"*** as "*a component of a product or of a system which fulfills a safety function for that product or system or the failure or malfunctioning of which endangers the health and safety of persons or property".*

It is not clear whether a "*safety function"* would also cover features related to safety or security but not actually safety-critical for the system. We believe that **this definition is too broad and that it should be focused appropriately on real risks to health and safety**. For products covered by the Union harmonisation legislation listed in Annex II, the definition of safety in the AI Act should designate the safety essential requirements defined in the EU harmonised safety legislation.

Article 3.33 defines ***"biometric data"*** as "*personal data resulting from specific technical processing relating to the physical, or physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."* This definition requires *"special technical processing"* but facial images do not require specific technical processing in contrast to, say, a facial vector computed based on a facial image. Biometric data is commonly understood to require going "beyond" what is perceptible to the naked eye. While facial images, standing alone, may be PII, they are not biometric. We suggest removing facial images to more precisely target biometrics in the framework of the regulation.

Finally, something that should also be clarified is whether the Regulation applies to **open source software (OSS).** This would be unfortunate because OSS is critically important to AI innovation, and **imposing conformity assessment requirements on OSS would have a chilling effect on open collaboration in the AI ecosystem.** In the same line, we believe that **general purpose AI systems should not be considered as having an intended purpose within the meaning of the AI Regulation.** We also recommend the Commission to clarify that placing on the market, putting into service or use of a general purpose AI system should not trigger any of the requirements under the AI Act.

With regards to the **scope,** Article 2 states that the Regulation applies to providers placing into service AI systems in the European Union, irrespective of whether those providers are established within the Union or in a third country; users of AI systems within the European

Union; providers and users of AI systems that are located in a third country, where the output produced by the system is used in the European Union. In the framework of the EU AI Act, all concerns and risks should be linked to how businesses use AI systems. Suppliers will not have visibility into the end use of AI systems, but those implementing/deploying the system for high risk use cases will. Furthermore, the Regulation does not contemplate third-party or vendor relationships in which a vendor/3PP is using an AI system on behalf of another party. **Article 2 of the AI Act should be clarified to limit the responsibility of suppliers as well as ensure that the territorial reach includes only those AI systems located in third countries that are used and pose potential risks within the EU itself, as opposed to other countries outside the EU.**

3. Prohibited AI practices

CCIA Europe recognises the importance of banning certain AI practices that represent a clear threat to the health and safety of humans and/or European values. When prohibiting AI use cases, policymakers must be very targeted to capture the specific uses of AI technology that they view as contrary to EU principles and not inadvertently sweep in other use cases. In the interest of legal certainty, **it is important that such prohibited practices are clearly defined so that acceptable AI practices do not risk falling into the scope of the ban.**

Article 5.a prohibits AI systems that deploy subliminal techniques *"beyond a person's consciousness in order to materially distort a person's behavior in a manner that causes or is likely to cause [...] physical or psychological harm".* **It is not clear what is meant by "*deploying subliminal techniques*", and "*psychological harm".*** CCIA Europe is concerned that this may be misread as a prohibition on the use and development of marketing, personalisation and search recommendations AI systems that, in some measure, use subliminal techniques to encourage customers to engage in commerce. However, this type of functionality neither causes physical or psychological harm, nor applies beyond consciousness since users always have to be informed when advertisement is displayed. **To support legal certainty, we recommend including a clear definition in Article 3 and Recital 16 and some references and criteria to better illustrate which type of systems are in scope of the prohibition.** In addition, and in order to better target policymaker's concerns, we recommend revisions to the language to reflect 1) the intended impact of the system and intentionality; 2) the limitation to implementation for use, and 3) the articulation of the materiality of the harm.

CCIA Europe also recommends to **elaborate on the ban on *"remote biometric identification system"* to clarify that this does not extend to any form of identity verification technology (facial recognition)** used in, for example, smartphones to verify the identity of a customer when processing an online payment. We agree that certain harmful AI practices should be prohibited whenever they contravene Union values, however, we warn against imposing a blanket ban on all facial recognition technologies

without taking into account that there are a diverse range of types and use cases and that these technologies can also be used to reduce risks (e.g. secure login on a smartphone).

Finally, the proposal also **prohibits AI-based social scoring for general purposes done by public authorities**. This prohibition is not absolute, social scoring is prohibited if it leads to unfavourable treatment because it is carried out in a context which is different from the one in which the data was originally collected and/or leads to unfavorable treatment that is unjustified or disproportionate to the social behaviour of natural persons or to its gravity. In principle, this prohibition is only targeted at public authorities. However, **we warn against expanding this prohibition to private companies as well.** The alternative conditions that the text proposes are too subjective and broad. This extension of the ban could affect, for example, insurance companies that deploy scoring systems to make important decisions based on people's behaviour (e.g. the reliability of a potential borrower of a loan). This could also affect sharing economy systems such as delivery services that use some kind of scoring system that evaluates the participants in the service. Companies automate their processes in order to be more effective and accurate in their decisions. We do agree that automation should not become a black box process, for this reason, **instead of directly banning any kind of scoring system, companies could provide customers with an understandable justification of why their rating has been declined,** for example, access to a loan.

4. High-Risk AI systems

Like any other technology, risks lie not in the AI application itself, but in its usage. Given that there is no risk inherent to a technology, CCIA Europe, therefore, supports a regulatory focus on "high risk" use cases to address specific and known risks and harms. We support the Commission's risk-based approach and limiting the focus to those uses that have significant impact on fundamental rights or cause health and safety concerns. However, our main concerns relate to the very broad definition of these uses in Annex III, as they may lead to including very broad categories of use cases in the scope of the regulation. **The way in which "high-risk" is predetermined in the current draft may have negative effects on innovation, jeopardise legal certainty and create a burdensome pre-approval process for likely already heavily regulated systems or products.**

Whether an AI system qualifies as "high-risk" should be based on its foreseeable impact on individuals, and the capacity of the AI system to make final decisions that create material adverse risk to a person's fundamental rights or health and safety. This differentiation is important from a policy perspective as AI may play a low-risk role in a high-risk category. For example, many low risk use cases may occur in the course of employee recruiting. A recruiter could use the AI search function on a job website to discover possible candidates who are looking for a new role (with their status set to "seeking opportunities" or "open to

new jobs"). A company could also interview candidates via video conferencing software that uses AI-developed background noise dampening to drown out traffic sounds, or convert a PDF job posting to a word document using AI-enabled OCR technology. In these cases, as well as others, use of AI that is not core to the task and is not used to make final decisions should not be regulated as high-risk AI systems. We therefore recommend that the wording in Article 6 (Classification Rules for High Risk AI Systems) and Article 7 (Amendments to Annex III) be revised to ensure clarity that an **AI system must also make final decisions that create a material adverse risk to a person's fundamental rights or health and safety.**

Accordingly, before providing a predetermined and prescriptive list of "high-risk" AI use cases, we recommend co-legislators to first undergo an in-depth analysis of the specific AI system following a case-by-case contextual assessment. Mandating specific requirements for use of AI techniques across use cases require cautiousness. For example, it may be appropriate to establish safeguards such as requiring human review, appropriate signage and notice, or record-keeping for a specific use case, but requiring a broader category of use cases to meet these requirements would be too inflexible in a dynamic and rapidly advancing area of technology. Proposed safeguards should be specific to a use case. **Rather than taking a blanket approach, we recommend that the AI Act follows a proper risk assessment for determining when a particular AI use case poses a "high risk" to the health, safety and/or fundamental rights and freedoms of the individual, and where AI systems are specifically playing a critical, high-risk role.**

Annex III (High-Risk AI systems referred to in Article 6) lists **biometric identification and categorisation of natural persons and management and operation of critical infrastructure** as ''high-risk''. We agree that some use cases of biometric identification could be considered high risk, and therefore warrant mandatory requirements. However, not all uses of biometric identification pose a risk to fundamental rights, biometric technologies can be also used for specified safety, security, fraud, and compliance purposes. In this regard, we suggest for technical accuracy reformulating this article clarifying that biometric identification of natural persons will be considered as ''high-risk'' when they do not express or imply agreement. In addition, the management and operation of critical infrastructure should not be regulated as a high-risk AI system, but rather the AI systems in the critical infrastructure themselves.

While the Commission text correctly exempts scenarios when users have agreed to be identified, that agreement can be manifested through conduct, and not just words (for example, by trying to enter a building with a biometric ID system). Following the same argument we stated in the previous section, **we would caution against including all types of biometrics and its various use cases into a single category, but rather assess the actual impacts of this technology, how it is being used in various circumstances and consider possible risk management measures.**

The Commission lists in Annex III of the Regulation examples of high risk AI use-cases that will be subject to the highest level of obligations. In addition, the Commission will have the power to expand such a list by delegated acts, as use-cases of AI continue to develop and risks evolve. When updating the list, **it is key to avoid unintended inclusion of AI systems that do not pose any substantive risk.** The aim of the mechanism that the Commission proposes is to keep up with the technological developments, we do agree with the need for the Regulation to be future-proof, however, to support legal certainty and market predictability, **we recommend the Commission to involve stakeholders in any future process for updating the list in order to take an informed decision.** A clear procedure of the revision of Annex III would allow actors involved in the development of AI systems to anticipate legal developments that could impact these technologies.

5. Requirements for high-risk AI systems

In line with a risk-based approach, the proposal allows high-risk AI systems to be placed on the European market as long as they comply with a set of horizontal mandatory requirements for trustworthy AI and follow conformity assessment procedures. As currently articulated, **some of the requirements are too vague and therefore difficult or even impossible to implement and would require practical guidance to facilitate business compliance.** Many requirements also attempt to control actual development of the system rather than place safeguards around its use, which will limit ability to develop and innovate. This creates a high legal uncertainty for companies that will have to undergo lengthy, bureaucratic approval processes as well as carry significant costs and administrative burden that will impact the start-up ecosystem in Europe particularly. Furthermore, unless one entity is responsible for all aspects of the system, different groups in the chain of development, deployment, and use will have limited visibility and ability to meet the proposed requirements. Without any doubt, all this may severely impact European innovation in AI, keeping Europe behind the global AI race due to broad compliance measures. **We urge lawmakers to frame the mandatory requirements on high-risk AI systems in a way that is flexible and realistic to ensure their easy adoption by businesses. Moreover, these requirements would need to be adjusted to ensure that they reflect existing gaps in harmonised standards and are proportionate to the actual foreseeable risk to the individual to avoid creating an uneven playing field in the distribution of responsibilities between the different actors in the AI value chain.**

For example, Article 10.3, as currently drafted, requires that data sets are ''*free of errors and complete",* this requirement is largely unrealistic and subject to varying interpretations. In addition, it should be noted that while developers of AI systems often manage the data on which the system is initially trained, many systems ingest data from users as part of their operations, and whether and how that data is retained, used and deleted is often controlled

by the user of a system. This means that often the user, rather than the provider, is best placed to assess the error since the provider may not be in a position to verify. This is an example of the **need to revise requirements that target specific AI systems and desired outcomes and focus on placing safeguards around use of AI systems by addressing harms that cause concern, rather than designating prescriptive ways to achieve those outcomes or control AI development,** particularly in light of the fact that they may vary based on context and as the technology evolves. In the specific case of 10.3, the language as drafted is not feasible—it is impractical for a data set to be complete (more data is always available) or free of errors, and these requirements are unnecessary to achieve goals like appropriate representation.

Similar problems arise with other obligations and requirements, for example, Article 11 (technical documentation) and Article 13 (transparency to users) are overly broad and it is not possible for the provider alone to fulfill them. The provider can offer technical documentation about the development, training, and performance of the AI system, however, it should be noted that the data on how the system interacts and other relevant information would need to be supplied by the user itself so that the provider has complete information about the system.

The human oversight requirement from Article 14 is also overly ambitious. It requires ''*to enable the user to fully understand the capabilities*'' of the system. Providers can create mechanisms for incorporating human input and feedback and exercising oversight, however, for a proper oversight, users would need to be appropriately trained to use the system. Human oversight is a valuable risk management tool, but it will not be appropriate or necessary in all use cases or at all points in the AI system. For example, it is not clear what it would mean to oversee an AI system, however in some cases a human may review the outputs or recommendations of a system. The value and nature of human oversight will depend on the specific use case and risks. Similarly, Sections 3 and 4 are overly prescriptive for the same reasons. Section 5, which requires two human reviewers for biometrics identification, should be in addition either deleted or narrowly tailored to identification of persons that would have significant impacts on human rights or liberties.

Ensuring that systems are used in such a way that they achieve appropriate levels of accuracy, robustness and cybersecurity (Article 15) is highly dependent on the choices made by users of AI systems. Providers also often lack direct access to the system as deployed by their customer, meaning that they are unable to conduct post-market monitoring of the system's performance (Article 61). Finally, while developers would need to take effective measures to manage risks associated with the design of the system (Article

9), users are the only ones best fit to assess whether the mitigations put in place are appropriate.

Building on the above, and in conclusion, we recommend, in the overall revision of high-risk requirements, that:

1) **Requirements should be high level**, with details being driven by industry-specific regulators (e.g. medical device regulatory bodies should be responsible for establishing AI medical device requirements), or by broader standards bodies.
2) **Requirements should seek to avoid regulating input/development of systems,** which will significantly hamper companies' abilities to innovate and iterate, and instead focus on output, such as managing how the output is used to make decisions.
3) **Requirements should be objective driven and specifically address the risk of the use case**. For example, a 10-year records retention requirement should not be needed even for many high risk use cases, but only for situations where having records to consult would make a difference to fundamental rights/health and safety.

6. Obligations for providers and users

Chapter 3 places most of the obligations and undergoing conformity assessment on providers of high-risk AI systems. **The AI Act currently focuses too extensively on the responsibilities of AI providers when, often, AI users are best positioned to meet them. CCIA Europe believes that the distribution of the responsibilities across the AI value chain needs to be re-evaluated to ensure that compliance obligations are assigned to the actors that can most appropriately ensure compliance.**

For example, this would be the case of general purpose Application Programming Interface (APIs) and open-source AI models that are not specifically intended for high-risk AI systems, however, users could use it in a way that is considered as high-risk and therefore fall into the scope for compliance. However, the Proposal, as currently drafted, requires providers to be responsible for situations where they have little or no visibility or control over how the system is being used and lack the operational access to fulfill many of the requirements.

This case is somehow addressed in Article 28 which shifts obligations from the provider to the distributor, importer, user or other third party if they ''*modify the intended purpose of a high-risk AI system already placed on the market or put into service*'' or makes ''*a substantial modification to the high-risk AI system*''. However, this shift is limited to Article 16 and it is not clear if using a general-purpose AI system for high-risk use would be considered as

modification of the intended purpose and therefore the responsibility would shift accordingly.

For this reason, we recommend lawmakers to amend Article 28 so that it applies to users who modify the intended purpose of the AI system already placed on the market or put into service to create a high-risk AI system.

7. Enforcement

As currently drafted, monitoring and enforcement are the responsibility of the Member States, although the Commission has a role through the European AI Board by contributing to the effective cooperation of the national supervisory authorities and providing advice, recommendations and expertise. **CCIA Europe believes that it is necessary to have a clear delegation of duties between national authorities so that market participants have a clear understanding of which body is competent for their activity.**

8. Interrelation with other EU law

AI is already regulated in several policy areas, including the EU General Data Protection Regulation (GDPR). The GDPR already provides protection against the use of ''automated decision-making'' as well as a strong foundation for AI governance through its requirements around ''fairness'', ''accuracy'', ''transparency'', ''purpose limitation'', ''data minimisation'' and ''automated decision-making''. In order to provide legal clarity for users, consumers and companies, avoid duplication and conflicting obligations, **we recommend that the proposed Regulation is aligned with existing GDPR principles, terminology, definitions, risk assessment methodology, and other requirements that currently apply to the use of ''automated decision-making''.** Also we urge policy makers to consider the interplay between the AI Act and the currently considered review of civil liabilities for AI-enabled services and products. The AI Act aims at introducing safeguards that reduce risks for citizens. Potential future consumer harm and resulting claims become even less likely. **It is therefore not justified to introduce on top new burdensome AI-specific liability obligations.**