3 August 2021

Response of

ACT | The App Association
Rue de Trèves 45,
1040 Brussels, Belgium

to the

European Commission

to its

Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (AI Act) and amending certain Union legislative acts

ACT | The App Association feedback to the European Commission's proposal for a Regulation laying down harmonised rules on Artificial Intelligence (AI Act)

I. Introduction and statement of interest

ACT | The App Association (App Association) appreciates the opportunity to submit its views to the European Commission (Commission) on its proposal for a Regulation to lay down harmonised rules on Artificial Intelligence (hereafter AI Act) and amend certain Union legislative acts. The App Association represents thousands of small business software application development companies and technology firms that create the technologies that drive use cases in the internet of things (IoT) and across consumer and enterprise contexts. Today, the value of the ecosystem the App Association represents – which we call the app economy – is approximately €830 billion globally and is responsible for over 1.3 million jobs in the European Union (EU).[1] Alongside the world's rapid embrace of mobile technology, our members create innovative solutions that power IoT across modalities and segments of the economy. The Commission strategy and the numerous efforts concerning AI policy and regulation directly impacts the app economy and our members. We support the Commission's goal of promoting and incentivising advancements in technology and innovation while preserving European values, including privacy, civil liberties, human rights, the rule of law, and respect for intellectual property, as well as protecting economic and national security.

Some forms of AI are already in use to improve European consumers' lives today – for example, AI is used to detect financial and identity theft and to protect the communications networks upon which Europeans rely against cybersecurity threats. Moving forward, across use cases and sectors, AI has the potential to improve European consumers' lives through faster and better-informed decision making. However, AI also potentially raises a variety of unique considerations for policymakers.

Our members, and many other tech start-ups and SMEs, are at the forefront of innovation, constantly advancing new products and services. This creates an opportunity for the EU to develop a regulatory framework that incentivises further innovation while balancing the potential risks of AI. The App Association appreciates the Commission's efforts to develop a policy approach to AI that will bring its benefits to all, balanced with necessary safeguards to protect consumers. We encourage policymakers to consider the many angles and interests that AI impacts before making statutory or regulatory changes.

We share the Commission's goals of creating an ecosystem of trust and excellence and offer the initial suggestions below to ensure a balanced approach to achieve these objectives. The App Association thanks the Commission in advance for consideration of our feedback.

II. The proposal for the AI Act

a. Defining Artificial Intelligence under the Act

The App Association believes a clear definition of AI is necessary for developers. The Commission's proposal defines AI systems, rather than AI itself. Although it is based on the Organisation for Economic Cooperation and Development's approach, the Commission is taking a more vague and expansive approach. In Annex I, the proposal lists the computer science techniques and approaches that would fall under this definition, and Article 4 of the proposal

[1] https://actonline.org/wp-content/uploads/Deloitte-The-App-Economy-in-the-EU-2020.pdf

stipulates that the Commission can amend and update this list as technology advances. Currently, the list includes machine learning approaches, such as supervised, unsupervised and reinforcement learning, using several methods including deep learning. The Annex also enumerates various logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference, and deductive engines, (symbolic) reasoning and expert systems, as well as statistical approaches, Bayesian estimation, search, and optimisation methods.

The App Association believes AI is an evolving constellation of technologies that enable computers to simulate elements of human thinking – learning and reasoning among them. An encompassing term, AI entails a range of approaches and technologies, such as Machine Learning (ML) and deep learning, where an algorithm is based on the way neurons and synapses in the brain change due to exposure to new inputs, which allows independent or assisted decision making. AI-driven algorithmic decision tools and predictive analytics are having and will continue to have, substantial direct and indirect effects on Europeans. Today, Europeans encounter AI in their lives incrementally through the improvements they have seen in computer-based services they use, typically in the form of streamlined processes, image analysis, and voice recognition. We urge the Commission to consider these forms as 'narrow' AI. The App Association notes that this 'narrow' AI already provides great societal benefit. For example, AI-driven software products and services revolutionized the ability of countless Europeans with disabilities to achieve experiences in their lives far closer to the experiences of those without disabilities. AI will also play an essential role in self-driving vehicles and could drastically reduce roadway deaths and injuries. From a governance perspective, AI solutions will derive greater insights from infrastructure and support efficient budgeting decisions.

Given the above, the App Association believes that further clarity and narrowing is necessary regarding this definition to ensure predictability and sufficient legal clarity. The current list is overly broad and includes fundamental concepts like Bayesianism, which is foremost a mathematical theorem and could thus cover technologies that do not perform AI functions. Such a broad definition creates uncertainty for AI developers, providers, operators, and users. Concerning providers, we encourage the Commission to distinguish between roles across the AI value chain so that it is easy to determine which AI entities and systems are in scope. Such a differentiation would ensure that, for example, software libraries and toolkit developers are not considered 'providers'.

Considering the wide territorial scope of the AI Act, we also have concerns with the Commission's unilateral ability to amend and update the list of activities and approaches that fall under the AI systems definition. Further, the Commission gives no details on how it will make these updates and how often they can occur, which decreases businesses' ability to determine whether they are subject to the law. The Commission also should provide a clear pathway to assess overlap and/or conflict with existing Commission requirements, both cross-sectoral and sector-specific, that may already address what the Commission determines is an AI function. Considering that violators may face up to a €30 million fine or six per cent of their annual global turnover in fees, this uncertainty would be particularly devastating for SMEs and start-ups. Similarly, businesses that are covered by the law will likely have to comply with technical standards, and Article 41 of the proposal would allow the Commission to unilaterally adopt new standards where it finds existing ones insufficient. We strongly encourage the Commission to revisit this provision and instead commit to the multi-stakeholder and voluntary approach to standards development that the global community has established.

b. A risk-based approach

The App Association appreciates that in drafting the AI Act, the Commission has taken a risk-based approach. For businesses that develop and use AI, we agree with the Commission that trust is essential. The proposed risk-based approach aims to help establish trust by banning unacceptable AI use cases and significantly regulating others that carry substantive risks. Like the Commission, we also agree that a regulation that encourages trustworthy technology can increase both customer loyalty and the overall uptake of AI systems. However, as businesses that develop emerging technologies benefit from clear rules and the AI Act requires that 'high-risk' AI meet strict data governance and risk management standards, we believe that further clarification is needed regarding the definition of high-risk uses, and the responsibilities of AI providers, operators, and users. We also strongly encourage the Commission to, in exposing AI to new regulations, responsibly promote data access, including open access to appropriate machine-readable public data, development of a culture of securely sharing data with external partners, and explicit communication of allowable use with periodic review of informed consent.

The proposal distinguishes between minimal, limited, high, and unacceptable risks. While high-risk applications will have to comply with the obligations the Act lays out, the AI Act says little about the uses that are of limited risk or no risk at all. Greater detail is needed to differentiate between classes of risk and the obligations associated with them. Currently, the Commission only states that the minimal risk category means every existing AI system that is not explicitly discussed in the proposal. The App Association has concerns with this definition as it seems to cover the vast majority of AI systems in use in the EU. While these technologies may not be subject to explicit new legal requirements, the proposal (Article 69) encourages the adoption of codes of conduct for their regulation which may still shape their development even though they carry minimal to no risk. We agree that soft-law frameworks could foster transparency, human oversight, and robustness, but we encourage the Commission to promote the voluntary application of these principles.

The limited risk tier covers some high-risk technologies and some that aren't, requiring special transparency measures for deep fakes, AI systems that interact with people, and AI-powered emotion recognition systems/biometric categorisation systems. The App Association agrees that these AI systems may raise certain transparency issues and may need to be subject to special disclosures necessary to provide transparency and explainability and that those developing, offering, or testing AI systems should be required to provide truthful and easy to understand representations regarding intended use and risks that would be reasonably understood by those intended, as well as expected, to use the AI solution.

While only some AI systems with increased or higher risk levels will be subject to the legal requirements, the Commission does not differentiate between high-risk AI use cases and AI research and innovation in high-risk fields. If the AI Act is used to unduly restrict such research, it would be highly detrimental to the EU's overall potential to become a leader in AI, which is one of the Commission's goals for 2030. We, therefore, encourage the Commission to exempt research in high-risk fields from the AI Act's requirements consistent with ethical and legal norms. Determining boundaries of how and why businesses can use AI systems is important, but the boundaries should not unduly hamper the innovation they try to promote.

Further, the high-risk tier distinguishes between two kinds of AI systems: those embedded in products that are already subject to third-party assessments and those that are not embedded in

other products. The Commission considers the stand-alone AI systems high-risk when they are used in certain areas, but we also urge the Commission to consider the specific use case, rather than just the area in which the AI system is used as the use can significantly impact the risk profile. A wholesale categorisation of, for example, HR applications as high-risk will ignore that some HR uses that present little or no risk are subject to high-risk treatment, defeating the intent of a scalable risk-based approach the Commission aims to use. The Commission should thus clarify and tighten the definition of high-risk use cases to ensure that it only captures those systems that actually create significant risks, and to discard its approach to assessing risk for overly broad categories of use that do not allow a scaled approach to risk assessment. Additionally, as defined in Article 9, the 'safety component' of a product could cover any piece of, e.g., a regulated medical device or piece of machinery. We urge the Commission to narrow this definition and to distinguish between 'reasonably foreseeable' risks and 'risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse' (Article 9). Additionally, we encourage the Commission to make its process of amending the list of high-risk areas under Article 7 more inclusive of impacted stakeholders and to specify how such amendments will be determined in practice.

The AI Act proposes a highly complex regulatory system under which national governments can designate various 'supervisory authorities', 'notifying authorities', and 'market surveillance authorities'. While we support timely reporting of adverse events to relevant oversight bodies for appropriate investigation and action, the AI Act does not lay out obligations for the Member States or these authorities to coordinate in the interpretation and enforcement of the new rules. This is concerning to the App Association as it could create significant legislative fragmentation and make compliance immensely difficult for smaller AI companies. Establishing several new institutions on top of current laws governing AI, rather than leveraging current rules and regulators, by adding compliance burdens and delays, will likely slow down the development and use of new AI products and services. We urge the Commission to minimise regulatory overlap and ambiguity and maximise regulatory coherence and coordination. Regulatory coherence is especially important as it remains unclear how the AI Act will integrate with the General Data Protection Regulation concerning the processing of sensitive data.

Further, it will be critical to the success of AI and the Commission's goals to promote many of the existing and emerging ethical norms, particularly those addressing higher risk use cases (e.g., healthcare) for broader awareness and adoption by technologists, innovators, computer scientists, and those who use such systems. AI will only succeed if it is used ethically. The App Association believes that the Commission's framework for AI should ensure that AI is safe, efficacious, and equitable by:

- Urging AI developers to align with all relevant ethical obligations, from design to development to use, and encouraging the development of new ethical guidelines to address emerging issues with the use of AI as needed;
- Strive for consistency with international conventions on human rights; and
- Ensure that AI is inclusive such that AI solutions beneficial to consumers are developed across socioeconomic, age, gender, geographic origin, and other groupings.

The Commission can also accomplish many of its goals by promoting thoughtful design principles. The App Association supports requiring reasonable steps to be taken by developers to ensure their design of AI systems to be informed by real-world workflow, human-centred design and usability principles, and end-user needs. However, to accomplish this goal, the design, development, and

success of AI need to leverage collaboration and dialogue between consumers, AI technology developers, and other impacted stakeholders to have all perspectives reflected in AI solutions. We strongly encourage the Commission to ensure its restrictions on AI do not impede developers' ability to thoughtfully design their AI innovations.

c. Obligations for high-risk AI systems

For AI systems the Commission deems as high-risk, the proposal would implement various requirements concerning the testing, training, and validation of algorithms, ensuring human oversight, as well as meeting accuracy, robustness, and cybersecurity standards. Before entering the European Digital Single Market (DSM), businesses of all sizes would have to demonstrate conformity with these obligations. While we support the Commission's goal of fostering trust and boosting Europe's competitiveness, we believe these requirements may have negative unintended consequences and will ultimately hamper the Commission's goals.

The proposal suggests implementing a Conformité Européenne (CE) marking process, which companies receive once their AI system meets the safety, health, and environmental protection requirements laid out in the proposal. Only once the CE process is complete can an AI system enter the European market. While we appreciate that AI providers can mostly comply with these requirements through a self-assessment procedure, we still believe they are too burdensome for SMEs and start-ups. For one, we believe that the conformity assessment procedures should consider the limited resources of new and smaller players. They will face significant difficulties in affording to wait for the completion of a lengthy approval, and we encourage the Commission to implement a maximum timeframe of four weeks for authorities to approve a CE mark. To minimise unnecessary burdens on AI that is not high-risk, we also urge the Commission to consider self-declarations of conformity, paired with market surveillance and a requirement that adverse events be timely reported to relevant oversight bodies for appropriate investigation and action, to appropriately minimise compliance burdens and delays while speeding time to market.

Further, the data and data governance obligations require businesses to develop AI systems with relevant, representative, error-free, and complete data. The App Association supports good data management practices, but legally requiring businesses to ensure error-free data for AI training is not technically feasible. We strongly encourage the Commission to revise this provision to ensure more practical and effective data governance obligations. Instead, the Commission should consider requiring a reasonable effort to develop AI systems with relevant, representative, error-free, and complete data. The errors and inherent bias in all data will remain one of the more pressing issues with AI systems that utilise particular machine learning techniques. Because the App Association agrees that these data provenance and bias issues must be addressed, we support the Commission (1) requiring reasonable steps to identify, disclose, and mitigate errors and biases in AI datasets while also encouraging access to AI databases and promoting inclusion and diversity in data; and (2) requiring developers to take reasonable steps to ensure that data bias does not cause harm to consumers.

We also have concerns regarding the transparency requirements to disclose information about the characteristics, capabilities, and limitations of the AI system; the system's intended purpose; and information necessary for its maintenance and care. European regulators should not have broad authority to demand access to businesses' data, source code, or algorithms. We strongly urge the Commission to implement sufficient safeguards regarding the circumstances under which such information would have to be disclosed to protect valuable intellectual property, trade secrets, and

cybersecurity. Without such safeguards, investments in European data and data-driven innovations will decrease. We suggest providers be given the right to challenge access requests on the grounds of necessity and proportionality or intellectual property protection.

Similarly, the accuracy, robustness, and cybersecurity obligations are unclear regarding what constitutes the appropriate levels for AI systems and how appropriateness would be assessed. The requirements call for accuracy metrics without specifying them, and we strongly urge the Commission to further develop these obligations and clarify them sufficiently so that businesses can be sure they are following them correctly.

The requirements also call on providers of high-risk AI systems to establish extensive technical documentation for traceability and audit purposes. This documentation should contain compliance information concerning the other requirements, including data management practices, risk management systems, and automatic recordings (logs) of events/incidents. The App Association agrees that AI developers should consistently utilise rigorous procedures and must be able to document their methods and results and that AI should be auditable, validated where appropriate, and explainable. However, the extensive documentation requirements proposed by the Commission may force companies to unnecessarily increase administrative burdens and potentially force developers to reveal confidential information and will likely not be feasible for small companies operating in the high-risk space. Further, Article 9 does not explicitly specify the types of risks that providers should consider when taking risk mitigation steps.

While we support the introduction of regulatory sandboxes for AI systems in Europe for start-ups and SMEs, the App Association has grave concerns that the high-risk requirements are overly burdensome for SMEs. Sandboxes should not be the only guarantee of legal certainty for high-risk AI innovators. Further, we urge the Commission to ensure that Member States harmonise and implement a sandbox framework across the DSM.

Overall, the proposed requirements do not sufficiently consider the time and monetary restrictions small AI businesses face. According to the European Commission, a quality management system could cost businesses between €193,000 and €330,000 upfront and another €71,400 in yearly maintenance costs and could cause profits to decline by 40 per cent.[2] This is not a realistic cost for SMEs and start-ups which are often at the forefront of AI innovation. Additionally, according to a study by the Center for Data Innovation, the AI Act will cost the European economy €31 billion over the next five years and reduce AI investments by almost 20 per cent.[3] Unless it is significantly revised, the App Association believes the proposed requirements could significantly disincentivise start-ups, SMEs, and even larger players from developing innovative AI systems in Europe.

d. Unacceptable risk applications

Article 5 of the proposed AI Act prescribes a blanket ban on certain uses and fields of AI, including social scoring, dark-pattern AI, manipulation, and real-time biometric identification systems. The App Association believes that banning entire areas from being able to use AI doesn't align at all with a scaled risk management approach and strongly discourages the Commission from moving forward with this provision. Such bans do not signal that the Commission wants to enable innovation and progress in AI and may decrease investment and research into AI in the EU overall.

[2] https://digital-strategy.ec.europa.eu/en/library/study-supporting-impact-assessment-ai-regulation
[3] https://www2.datainnovation.org/2021-aia-costs.pdf

A scaled approach can reflect the Commission's vision to protect fundamental rights by allowing for some appropriate uses without banning entire uses and fields of AI. The examples the Commission lists in the proposal such as social scoring, techniques that can 'materially distort' a person's behaviour or 'manipulate' a person based on their age or physical or mental disability deserve special scrutiny. However, the Commission does not, for example, consider AI tools that are meant to assist those with disabilities which may be considered to 'manipulate' input to assist the user. We believe this definition of the banned AI systems needs a reasonableness standard for those users who can minimise risk based on their knowledge, and the ability to mitigate those risks.

Concerning dark patterns, they remain an elusive concept to define and arguably include a far greater range of players than currently recognised. Dark patterns are by no means a design tactic relegated exclusively to the domain of cutting-edge start-ups or mobile applications. Researchers found inconsistent and at times misleading user opt-out controls for email communications within a sample of 150 websites drawn from Amazon Alexa's ranking of the global top 10,000 websites. The list includes websites from industries as diverse as finance, health, media, and sports, and of varying sophistication and user design prowess.[4] We must also recognise that dark patterns are extensions of tactics used in the physical world. Design choices can require users to take exhaustive steps to effectuate a preference that may conflict with the businesses' preferences. As an example, when examining the email opt-out procedure at the *New York Times*, Cranor and Habib found that 'deleting the data they'd gathered on us required completing 38 different actions, including finding and reading the privacy policy, following a link to the data deletion request form, selecting a request type, selecting up to 22 checkboxes, filling in eight form fields, selecting four additional confirmation boxes, and completing an "I am not a robot" test.'[5] In the physical world, casino designers, for example, are notorious for constructing floor plans that intentionally disguise exits to manipulate guests into spending extra time within the facility. Few would call that a dark pattern, yet it seems equally manipulative to the opt-out practices at the *New York Times*. It might also be more useful to think of dark patterns as design choices in any type of business-to-user interaction that causes the consumer to purchase or sign up for things they didn't mean to. Insofar as the Commission seeks to bolster its monitoring of the marketplace for examples of dark patterns, it should remain aware that the practice is widespread, cross-cutting between industries, and endemic to many types of communication technologies, and not exclusive to AI applications.

Clearly, part of the issue in defining dark patterns stems from an ongoing migration of markets from analogue to digital spaces, across industries. Some dark patterns, such as 'confirm-shaming', are holdovers from longstanding face-to-face sales tactics in which salespeople employ behavioural nudges to close a sale or upsell a service.[6] Confirm-shaming, as currently understood, could include a prompt as simple as 'are you sure you wish to opt-out', a necessary piece of developer due diligence that could be construed as guilting a customer.[7] As with such sales tactics, confirm-

[4] Lorrie Cranor and Hannah Habib, "An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites", Soups 2019, August 2019. https://www.usenix.org/system/files/soups2019-habib.pdf
[5] Lorrie Cranor and Hannah Habib, "It's shockingly difficult to escape the web's most pervasive dark patterns", Fast Company, November 4, 2019. https://www.fastcompany.com/90425350/its-shockingly-difficult-to-escape-the-webs-most-pervasive-dark-patterns
[6] Harry Brignull, 'Types of Dark Patterns.' https://www.darkpatterns.org/types-of-dark-pattern8
[7] Harry Brignull, 'What are Dark Patterns.' https://www.darkpatterns.org/7

shaming should be understood to encompass a wide range of activities that run from innocuous to outright deceptive, the latter of which should be the main source of attention from regulators. While certainly starker when presented plainly on a website or app than when spoken aloud in a sales context, such a prompt hardly seems out of place in the broader marketplace and surely does not constitute an unfair or deceptive trade practice.

The App Association would urge the Commission to focus its attention and a potential ban only on examples of dark patterns that deceive and bring harm to a user. While there is a great opportunity to clarify and rid the market of harmful practices, an ambiguous or overinclusive definition or a blanket ban of dark patterns may harm app developers who are simply seeking to do the right thing.

III. Conclusion

The App Association appreciates the Commission's consideration of the above views. AI offers immense potential for widespread societal benefits, which is why the Commission should foster investment and innovation in any way practicable. Our members both use and develop solutions that include AI, and those are in turn used by countless Europeans. As society moves to adopt these technologies on a greater scale, it is important that the small business developers who power the €830 billion global app economy can contribute to this important trend. Since the proposed regulation applies to every high-risk AI system on the European market and will impact developers everywhere, we urge the Commission to design a regulation that is both understandable and feasible for SMEs and start-ups.

The AI Act should be future-proof and incentivise innovation, research, and development in the AI space for both low and high-risk systems across the EU. Therefore, we believe the Commission should reconsider some of its obligations on high-risk AI systems as well as the bans on 'unacceptable risk' AI systems. We thank the Commission for its consideration of our views and remain at your disposal for further engagement.

Sincerely,

Mike Sax
Founder and Chairperson

Brian Scarpelli
Senior Global Policy Counsel

Anna Bosch
EU Policy Associate