Consumer Technology Association™

1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

August 5, 2021

Consumer Technology Association
Comments on

European Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence and Amending Certain Union Legislative Acts

The Consumer Technology Association ("CTA") ®[1] respectfully submits these comments in response to the European Commission's ("Commission") "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts" COM(2021) 206 final (rel. 21.4.2021).[2]

CTA applauds the Commission's thoughtful framework set out in the Proposed Rules. While detailed and attentive to important considerations, the framework should be revised and recalibrated to reflect a more graduated approach which relies upon industry standards and consensus-based best practices, and a more nuanced framework that explicitly balances costs of over-regulating against the benefits of innovation in the emerging AI markets.

OVERVIEW AND SUMMARY

Along with the Commission, CTA has a significant interest in ensuring consumers in the European Union benefit from the promise of trustworthy and safe AI-enabled products and services. To that end, the Commission should proceed with policies that recognize the potential with which AI products and services can improve the lives of citizens in EU Member States. Such recognition is only possible through an AI framework that is not only consistent with

[1] CTA® is the tech sector. Our members are the world's leading innovators—from startups to global brands—helping support millions of jobs. CTA owns and produces CES®—the largest, most influential tech event on the planet.

[2] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM(2021) 206 final, 2021 ("*Proposed Rules*").

Producer of CES

sectoral legislation and existing regimes, but also commensurate with the evolving and innovative nature of the technology itself. While CTA is encouraged by the Commission's use of a risk-based framework in the Proposed Rules, ambiguities in the Proposed Rules as written could undermine or impair further innovation and development of this transformative technology. To address these concerns, CTA recommends greater clarity by the Commission, specifically regarding the portions of the Proposed Rules discussed herein.

CTA applauds the Commission for considering the potential costs of complying with this broad new regulatory framework, but CTA is concerned that the full impact of such costs may not be fully appreciated. Indeed, a recent study by the Center for Data Innovation indicates that such costs are likely to be much greater than the Commission estimates. The Commission must recognize that if compliance costs outweigh the benefits of the Proposed Rules, promising AI products and services may not be developed at all if the Proposed Rules force companies to assume exorbitant compliance costs in connection with conducting conformity assessments, recordkeeping, reporting and other duties. The Commission must be mindful of the potential impact not only on small- and medium-sized businesses, but on the EU market as whole.

Respectfully, CTA urges the Commission to address several ambiguities in the Proposed Rules. For instance, CTA recommends clarification of the definitions of "artificial intelligence" and "safety component." Also, clarifying the meaning of "provider" is critical for legal certainty, given the potential extra-territorial reach such ambiguity presents. Further, it is also imperative that the Commission review and revise the scope of certain requirements imposed, including those related to data governance, human oversight, recordkeeping and reporting. As discussed more fully below, these changes are necessary to ensure that the Commission's proposal leads to a balanced, risk-based framework that does not hamper innovation or the potential of this truly life changing technology.

TABLE OF CONTENTS

I. INTRODUCTION

The European Commission's ("Commission") work to put forward harmonized rules on artificial intelligence and machine learning systems marks an important step forward in the global policy debate over the development of appropriate frameworks to enhance and expand the availability and accessibility of trustworthy AI systems. This builds upon the already robust and effective set of best practices, principles and guidelines adopted in this industry to help guide the path towards the development of transformative and trustworthy AI. Indeed, AI has already offered immeasurable benefits to society and continues to introduce new innovative tools, applications and systems that are making our lives safer, more efficient and more fulfilling.

Indeed, during the global COVID-19 pandemic, AI is driving important research and testing necessary to defeat the virus. For example, French AI company Iktos has partnered with SRI International, based in Menlo Park, to discover and develop new anti-viral therapies using deep-learning models,[3] and healthcare providers in New York have developed AI algorithms that can predict whether a COVID-19 patient is likely to suffer adverse events in the near future.[4]

CTA applauds the Commission's thoughtful framework set out in the Proposed Rules. While detailed and attentive to important considerations, the framework should be revised and recalibrated to reflect a more graduated approach which relies upon industry standards and consensus-based best practices, and a more nuanced framework that explicitly balances the costs of over-regulating against the benefits of innovation in the emerging AI markets.

II. GENERAL COMMENTS

A. Compliance Costs are Likely to Hamper Innovation and Reduce Competition

While CTA applauds the Commission for its work in this space, the scope of new obligations under the Proposed Rules will be very significant and quite costly and will have a disproportionate impact on small and medium sized enterprises ("SMEs"). Indeed, by the Commission's own estimation, the costs of complying with the numerous new obligations proposed by the Commission will be equal to hundreds of thousands of dollars –a cost that is

[3] *Iktos and SRI International Announce Collaboration to Combine Artificial Intelligence and Novel Automated Discovery Platform for Accelerated Development of New Anti-Viral Therapies*, Drug Discovery Online (Mar. 4, 2020).

[4] *Coronavirus Tests the Value of Artificial Intelligence in Medicine*, Fierce BioTech (May 22, 2020); Farah Shamout *et al.*, *An artificial intelligence system for predicting the deterioration of COVID-19 patients in the emergency department*, 4 NPJ Digital Medicine 80 (2021) (proposing data-driven approach for automatic prediction of deterioration risk using a deep neural network that learns from chest X-ray images and a gradient boosting model that learns from routine clinical variables); Yazeed Zoabi *et al.*, *Machine learning-based prediction of COVID-19 diagnosis based on symptoms*, 4 NPJ Digital Medicine 1 (2021) (establishing machine-learning approach that trained on records from tested individuals and model that predicted COVID-19 test results with high accuracy using only eight binary features).

likely to cripple SMEs[5] and constitute a significant new burden for larger organizations. The resources diverted to complying with these rules will take away from that which may have otherwise been focused on investing in research and development to make these systems more accurate, efficient and safe. Further, SMEs burdened with high compliance costs may be forced out of the market, thereby reducing competition. In short, the compliance costs are likely to stifle innovation and undermine competition.[6]

According to the recently released study by the Center for Data Innovation, the Proposed Rules "will cost the European economy €31 billion over the next five years and reduce investments by almost 20 percent."[7] The CDI study warns of compliance costs for regulating Artificial Intelligence, in particular a "European SME that deploys a high-risk AI system will incur compliance costs of up to €400,000 which would cause profits to decline by 40 percent."[8] Further, the cost of obtaining an external conformity assessment can be up to €1 million.[9]

Complex and costly new mandates under the Proposed Rules are numerous. For example, Title III, Article 17 requires developers of "high-risk" AI systems to set up and maintain a "quality management system."[10] This requirement is among many new mandates with which, collectively, it will be very costly to comply. Additionally, the new proposed duties to maintain technical documentation and record-keeping will require covered providers to maintain an extensive amount of up to date technical documentation of high-risk AI systems[11] and generate numerous logs for duration of use, databases referenced, input data and humans involved in verification.[12] Further, the obligation to undertake conformity assessments will require providers to undertake extensive work necessary to certify completion of a regulatory assessment demonstrating compliance with the Proposed Rules before placing the AI product or system on the market.[13]

By the European Commission's own calculation, the estimated cost to set up a "quality management system" could be as much as €400,000.[14] The Commission specifically notes that this estimate is not inclusive of all anticipated costs such as the "costs of external legal advice and consultancy fees"[15] – which are likely to be significant given the length, complexity and consequences of non-compliance. Yet, the Commission also recognizes that companies are likely to incur significant legal and consultancy fees because such costs "inevitably vary with a

---

[5] The European SME Alliance has explained that main barriers to AI adoption are a lack of capital, lack of skills and inability to access sufficient data for training. *See* SME White Paper.
[6] *See* Benjamin Mueller, How Much Will the Artificial Intelligence Act Cost Europe?, Center for Data Innovation (2021) ("We estimate that the Artificial Intelligence Act would cost European businesses €10.9 billion per year by 2025, having cost the economy €31 billion by then. This excludes the opportunity cost of foregone investment into AI.").
[7] *Id*. at p. 4.
[8] *Id*.
[9] *Id*. at p. 8.
[10] Proposed Rules, Title III, Art. 17.
[11] *See id*. at Title III, Arts. 11, 18.
[12] *See id*. at Art. 12.
[13] *See id*. at Title III, Arts. 11, 18 (technical documentation), Art. 12 (record-keeping), Art. 19 (conformity assessments).
[14] European Commission, Study supporting the impact assessment of the AI regulation, p. 152 (Apr. 2021).
[15] *Id*. at 13.

company's size and preferences" as well as "the complexity and stringency of the regulatory requirements in the proposed regulation."[16]

Requirements for certifying compliance, and providing assurances that AI products or systems will remain compliant, will increase providers' costs and create hurdles to innovation. Resources spent on compliance cannot be put to research and development of new technology and tools. While CTA agrees that appropriate oversight is important, it should be developed in a manner that will not unreasonably add to providers' costs and potentially undermine innovation and technological advancements.

Targeted relief or carve-outs for smaller entities should be considered. The Commission acknowledges that the objectives of regulatory sandboxes should be, in part, "to accelerate access to markets, including by removing barriers for small and medium enterprises (SMEs) and start-ups."[17] For example, Title V encourages national authorities to set up regulatory sandboxes and consider SME interests related to conformity assessments when setting fees.[18] Yet there is insufficient empirical support to rely on the introduction of regulatory sandboxes *alone* to mitigate the regulatory impact on smaller entities.[19] Feasibility assessments of regulatory sandbox execution plans at the outset and at periodic intervals thereafter is a critical step to ensure the Member States are accountable to industry and to consumers.[20] Also, the potential patchwork that may result from mere encouragement of sandbox development to support SMEs could dampen innovation and create burdens for SMEs developing AI systems in various Member States with less sandbox support.[21]

Given the Commission's estimated compliance costs, coupled with the likelihood Member States offer uneven sandbox support, the costs of compliance for new entrants and SMEs will be prohibitively expensive. That will, in turn, limit new market entry and stifle innovation. For these reasons, the Commission should consider pulling back on several of its most costly new mandates, including those described herein.

B. Extra-territorial Reach of Proposed Rules is Problematic

As proposed, the Proposed Rules apply to AI systems and users of AI in the European Union, as well as providers and users of AI *beyond* the European Union "where the output produced by the system is used in the Union."[22] The reach and scope of these rules is incredibly broad, especially considering that the unique "value chain" in the AI sector includes many developers, programmers and service providers that may or may not be located in the EU, and who may or may not have any responsibility for placing the final products on the market.

Further, the Commission's proposed penalties for noncompliance and confidentiality protections exacerbate the potential harms of the Proposed Rules' extra-territorial reach. Proposed penalties would authorize regulators to impose fines up to €30m or six percent of "total

---

[16] *Id*.
[17] Proposed Rules, Recital (72), p. 34.
[18] *See id*. at Title V, Art. 53 (sandboxes), Art. 55(2) (fees), p. 71; *see also*, Title V, Art. 43.
[19] *See* Appaya and Haji, Four years and counting: What we've learned from regulatory sandboxes, World Bank Blogs (Nov. 2020).
[20] *Id*.
[21] *See* Proposed Rules, Recital 72, p. 34; *see also*, Recital 10, p. 20.
[22] *Id*. at Recital 11, p. 20.

worldwide annual turnover for the preceding financial year, whichever is higher."[23] As currently framed, such fines could reach revenue generated from services and applications *outside* of the EU. For example, a US-based AI platform could be made available wholesale in the industry to aid other companies in developing software or deploying machine learning models in the cloud. These "wholesale" AI services offer pre-trained models that are capable of undertaking different tasks (analytics, insights, or recommendations) of general application. Notably, many customers will then take these general wholesale models and conduct further model training for specific use cases. The customer then places the model on the market, often without the knowledge of the "wholesale" provider. If a customer takes the platform and creates an AI product or system that is ultimately sold or used in the EU, and under a broad reading of these rules, the US-based platform wholesaler could fall under the Proposed Rules.

Entities like the US-based wholesaler should not be subject to an expansive regime with far-reaching consequences and costly mandates that could inhibit innovation and development. The extra-territorial reach of the Proposed Rules raises questions about whether companies might have to stand up two different versions of an AI product or system in the US and EU. Or, for companies leveraging AI systems across the EU and those developing AI products or systems in the EU for multiple countries, the extra-territorial reach of the Proposed Rules raises questions about whether substantial requirement buildouts could be necessary.

Although similar penalties exist in other laws (e.g., GDPR), the potential reach of applications along the supply chain in this instance are broader. The Commission recognizes that the AI supply chain is multi-faceted and involves numerous entities involved in developing systems and applications. As the Commission explained, the value chain includes entities "involved in the sale and the supply of software, software tools and components, pre-trained models and data, or providers of network services…"[24] But, as explained above, some of these entities will not be operating in the EU or have any responsibility for placing AI products or systems in the EU marketplace. Like upstream suppliers, they will merely be providing inputs, or components, of such systems but will have no authority or control over the final product placed on the market. As a result, they should be free from any potential liability and the consequences of non-compliance of any specific AI product or system that they do not control. It is unjust and unreasonable for the Commission to expect supply chain providers to be liable for products or systems that they have no control over – for both EU and non-EU suppliers.

Ultimately, the root of the issue is the ambiguity of who is covered (i.e., the meaning of "provider" and "output"), which compounds the issue of the Proposed Rules' extra-territorial reach. The Commission recognizes the complexity of the AI value chain, made of "relevant third parties, notably the ones involved in the sale and the supply of software, software tools and components, pre-trained models and data, or providers of network services."[25] Yet the broad definition of "AI system" described above and subsequently of a "provider" pose serious challenges to determining which "AI systems" and which "providers" are within the scope of the Proposed Rules. For example, entities developing toolkits or software libraries should not be considered "providers." Rather, stating unequivocally that these relevant third parties are not considered "providers of AI systems" in the Proposed Rules is one way to distinguish such varied actors. The Commission should clarify the Proposed Rules to differentiate the roles

[23] *Id*. at Title X, Art. 71(3), p. 82. *See also*, Title X, Art. 71(4)-(5), p. 82.
[24] *Id*. at Recital 60, p. 32.
[25] *Id*.

across the AI value chain. Removing this particular ambiguity is at the core of the Proposed Rules' extraterritorial scope.

III. THE COMMISSION SHOULD CLARIFY THE SCOPE OF CERTAIN DEFINITIONS

A. Definition of "Artificial Intelligence" is Too Broad

As currently framed, the definition of the term "artificial intelligence system" is too broad.[26] Specifically, by incorporating certain techniques and systems in Annex I ("wide variety of methods" and "statistical approaches; Bayesian estimation; search and optimization methods") the definition captures numerous processes and systems that do not use AI or machine learning. Further, the definition is open ended and likely extends far beyond the intended scope, potentially reaching applications such as spam filters and consumer services like fraud detection.

How "artificial intelligence" is defined will have a foundational impact on how the Commission's AI regulations are implemented. If the concept of artificial intelligence is too broad, it will result in one size fits all regulation for all AI applications and "high risk" AI systems across sectors despite differences between the sectors and distinctions between the types of AI uses. For instance, risks posed by AI systems used in the transportation sector will necessarily differ from those posed by AI systems used in the financial, healthcare, or retail sectors.

The Commission recognizes the importance of accounting for the "specificities of each sector…without interfering with existing governance, conformity assessment and enforcement mechanisms and authorities established therein."[27] Yet, it remains unclear whether and to what extent the Proposed Rules would apply to existing sector-specific frameworks.

The Commission should utilize a definition of AI that narrowly focuses on those unique aspects of the technology (i.e., systems capable of learning), but which avoids capturing general concepts or constructs used in computer science (e.g., algorithms, statistical approaches) that do not themselves constitute AI. This can be easily achieved by using the definition set forth in the Commission's April 2018 Communication on AI.[28] Alternatively, the Commission should consider definitions devised by the High-Level Expert Group on AI.

B. Risk Classifications Should be Clarified

Risk classifications delineating between AI uses that are "high-risk," "low-risk," or "minimal risk" pose significant challenges for complying with the rules, as written.[29] Uncertainties stemming from this root ambiguity include the circumstances under which law

[26] Proposed Rules, Title I, Art. 3(1).
[27] Proposed Rules, Recital (29).
[28] "Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI- based systems can be purely software-based, acting in the virtual world (e.g., voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g., advanced robots, autonomous cars, drones or Internet of Things applications)." COM(2018) 237 Final, p. 1.
[29] *See* Proposed Rules, Title III Arts. 6-7, *see also*, Title III, Art. 13. Title IV, Art. 52.

enforcement is permitted to use certain AI products or systems[30] and the inclusion of AI products or systems that could cause harm that might be "immaterial."[31] For example, an online travel agency could be impacted by the applications affecting consumers rights or be required to apply "high-risk" rules based on use of creditworthiness in offering consumers particular options for travel financing. More specific definitions of risk classifications, and clarification as to which product "components" they apply, are needed.

Addressing the threshold risk classification will not cure all ambiguities throughout the Proposed Rules, but clarity in this regard is the critical base upon which the entire proposal rests. We recommend the Commission makes clear, with concrete use cases, what AI systems qualify as "high-risk" and "low-risk" or "minimal risk" – including whether transparency suffices to exclude AI systems from the scope of the Proposed Rules. In addition, the Commission should clarify as to which product components these risk classifications apply.

We also recommend the Commission clearly articulate what AI products or systems qualify as "high risk." Further, in so doing, the Commission should explicitly exempt products covered by existing laws from the "high-risk" category. This will be the most effective measure to cure confusion about what constitutes "high-risk" in terms of harmonization.

C. "Safety Component" Definition Should be Clarified and Harmonized

"Safety component of a product or system,"[32] as defined by the Commission, should be harmonized with existing European Union product safety laws because currently the Proposed Rules do not clearly establish a process for harmonizing existing consumer safety protections with the new obligations set forth in the Proposed Rules. As written, the Commission's definition situates "safety component" broadly in the context of products or systems affecting the "health and safety of persons and property."[33] At the same time, the Commission emphasizes the importance of harmonization throughout the Proposed Rules.[34] For instance, some of the Commission's objectives for harmonization are "to facilitate the free movement of products in the internal market and to ensure that only safe and otherwise compliant products find their way into the market."[35]

However, beyond consistent emphasis on harmonization, no obvious roadmap emerges between the Commission's concept of safety in the Proposed Rules and existing product safety laws in the European Union.[36] This is largely due to unclear or seemingly conflicting provisions

[30] Title II, Art. 5(4).
[31] Preamble (4).
[32] Title I, Art. 3(14) ("'safety component of a product or system' means a component of a product or of a system which fulfils a safety function for that product or system or the failure or malfunctioning of which endangers the health and safety of persons or property").
[33] *Id*.
[34] *See*, *e.g.*, Recital 2.1, 2.3, 2.4, 5.2.6, Preamble (5), (28), (30), (31).
[35] Recital 28.
[36] Art. II (2) ("For high-risk AI systems that are safety components of products or systems, or which are themselves products or systems, falling within the scope of the following acts, only Article 84 of this Regulation shall apply: (a) Regulation (EC) 300/2008; (b) Regulation (EU) No 167/2013; (c) Regulation (EU) No 168/2013; (d) Directive 2014/90/EU; (e) Directive (EU) 2016/797; (f) Regulation (EU) 2018/858; (g) Regulation (EU) 2018/1139; (h) Regulation (EU) 2019/2144."); Recital (29) ("…it is appropriate to amend those acts to ensure that the Commission takes into account, on the basis of the technical and regulatory specificities of each sector, and without interfering with existing governance, conformity assessment and enforcement mechanisms and authorities established therein,

in the Proposed Rules. Specifically, Title III, Article 6 (a) and (b) refer to the AI system itself as a product covered by legislation listed in Annex II,[37] and it is unclear whether this includes any product or only those products for safety. As a result, it is unclear which products are subject to which mandates. For instance, the Proposed Rules state that "it is appropriate to classify them as high-risk…if the product in question undergoes the conformity assessment procedure with a third-party conformity assessment body pursuant to the relevant Union harmonisation legislation."[38] Application of this provision alone requires clarification of the underlying concepts, particularly what is meant by safety and the scope of the product.

To unravel these complex provisions, concepts of safety should be unified and harmonized across other applicable legislation. Additionally, the scope of the product needs to be clarified to specify whether the definition is inclusive of all products or products for safety.

D. Scope of Biometrics Should be Restricted

As currently framed, the scope of biometric data is too broad and may capture, unintentionally, non-high-risk applications processing biometric data. Biometric data is defined as "personal data resulting from specific technical processing relating to the physical, 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."[39] This broad scope clearly reaches certain high-risk applications, including biometric identification and categorization of natural persons.

At the same time, the broad scope of biometrics also appears to reach more benign applications such as picture classification (e.g., photo album, photo storage and editing applications), as well as AR/VR images used in retail commerce or gaming. Other non-high-risk applications include detection software for digital still cameras and camcorders that optimize picture-taking (e.g., auto-focus, smile detection). Moreover, it appears that this broad scope would encompass safety measures such as body temperature estimation without identification (e.g., crowded scene visualization) for infection prevention or driver drowsiness detection.

But it is not at all clear that the Commission intends to reach non-high-risk applications like those described above. Indeed, the discussion in the Recitals seems to focus on the high-risk applications associated with biometric data (i.e., the use of such data in remote biometric identification systems).[40]

To resolve this ambiguity, the Commission should clarify the scope of biometrics and distinguish between high-risk and non-high-risk AI applications.

E. Application to Intended Uses of AI Systems is Inflexible

---

the mandatory requirements for high-risk AI systems laid down in this Regulation when adopting any relevant future delegated or implementing acts on the basis of those acts.").

[37] Proposed Rules, Title III, Art. 6(a)-(b).

[38] Recital (30) ("In particular, such products are machinery, toys, lifts, equipment and protective systems intended for use in potentially explosive atmospheres, radio equipment, pressure equipment, recreational craft equipment, cableway installations, appliances burning gaseous fuels, medical devices, and in vitro diagnostic medical devices.").

[39] Title I, Art. 3(33).

[40] *See, e.g.*, Recitals (7), (8).

The Proposed Rules impose certain obligations based upon the "intended use" or purpose of the AI systems or products, but this paradigm fails to recognize that many AI systems are only developed with general capabilities (e.g., computer vision or natural language processing) which are then further trained and tailored in order to serve specific "intended" use cases. Indeed, a natural language processing ("NLP") system or model may be developed with certain capabilities that could be used differently depending upon the specific intended use case (which could represent a range of potential applications). For example, an NLP that is trained to review and interpret text or data from an industrial system has very different risk factors from an NLP system that is trained to engage or interact with human beings (e.g., as a chat bot in a customer service role).

The Commission should acknowledge this distinction and distinct roles of providers in the AI value chain. Recognizing that many entities simply provide AI systems that serve as foundational tools for another entity to then use to address specific use cases is essential. Further, recognition of this distinction is necessary to ensure that the burden of compliance under the existing framework could have a severe impact on AI developers that are not putting services into the market, but that are only offering tools for other entities to integrate into services placed in the market.

F. Evolving Nature of Machine Learning Not Adequately Addressed

One of the most unique and important attributes of most machine learning models is that they evolve, expand and become more efficient and accurate over time as they gain access to additional data, undergo further training and "learn" about the data they analyze. When AI systems are trained on additional data, continuous learning and re-training lead to greater accuracy and performance. That system evolution should lead to more accurate predictions, recommendations and actions. However, the Proposed Rules do not appear to take into account the evolving nature of machine learning systems. Retraining models can improve model accuracy and continuously 'sharpen' the model.[41]

For example, Article 13 would require, in part, that high-risk AI systems be accompanied by instructions for use specifying "the changes to the high-risk AI system and its performance which have been pre-determined by the provider at the moment of the initial conformity assessment" and "any necessary maintenance and care measures to ensure the proper functioning of that AI system."[42] A machine learning model does not exist in a vacuum, and its performance depends not only on the data it uses to understand a problem, but also on changes to that data over time. This necessarily means that changes to the model are a function of the nature of the model.[43] Thus, if the model is performing as intended, it will change and evolve to reflect the access to broader data and datasets, which enhance accuracy. To comply with Article 13, then, would be to ignore that a snapshot of the model's performance speaks little of its overall health over time, as the model evolves and grows. Additionally, it is important to understand how a machine learning model is performing before determining its retraining needs. To provide information regarding the maintenance and care measures for proper functioning of the system similarly puts the cart before the horse.

[41] Andreas Spillner *et al.*, Software Testing Foundations, 4th ed. at pp. 169-203 (2014) ("Test Management").
[42] Proposed Rules, Art. 13(2)-(3).
[43] *See* Spillner *et al.*, Test Management, at pp. 169-203.

Likewise, Article 14 requires, in part, implementation of measures enabling human oversight to "be able to correctly interpret the high-risk AI system's output."[44] Interpreting the system's output requires continuous monitoring of prediction accuracy, which may require retraining over time. Requiring a human to monitor and manually determine when to re-train a model can be both costly and perilous given the potential for human error. Rather, investment in an automation system that re-trains based on evaluation of certain performance metrics or even re-trains at specified periodic intervals provide more reliable performance assessments.[45]

IV. THE COMMISSION SHOULD CONSIDER MODIFYING OR CLARIFYING KEY ELEMENTS OF THE PROPOSED RULES

A. Data Governance

Article 10(3) states that "training, validation and testing data sets shall be relevant, representative, free of errors and complete." This proposed standard is overly prescriptive and does not reasonably reflect the reality of existing data sets in the industry today. Further, even if these goals were achievable (which they are not), they would not ensure AI products or systems were free of adverse bias or outcomes. The Commission should reconsider this proposal and adopt a more flexible standard that encourages developers and providers to work towards the development of data sets that minimize error and maximize representation of diverse communities. As the industry works toward such data sets, the Commission should also support sound algorithmic principles to identify and mitigate potential risks of harmful biases resulting from data sets.

Data sets used to train AI products or systems vary widely in scope, content and origin.[46] Although some data sets are specifically developed to meet generally recognized principles of clarity, relevance and representativeness, not all data sets meet that objective. Data sets are sourced from a variety of databases and develop for numerous purposes which may, or may not, meet the aspirational principles of clarity, relevance and representativeness. Certainly, the industry should be moving toward the development and use of data sets that do meet those goals, but to mandate the use of only those data sets that are "complete" and "error free" would set an impossible standard. Finally, the proposal to mandate the use of "complete" data sets may conflict with GDPR regulations that prohibit developers from accessing sensitive PII and attributes such as gender, ethnicity or income levels.

This proposal is further burdened by the fact that there is no clear standard for what makes a data set complete or error free. Because society is so multifaceted and dynamic, there may be many ways to compile data in a manner that reflects specific attributes of a particular set of data. For example, where AI is used to predict anticipated maintenance requirements on medical diagnostic systems or equipment, what constitutes a complete or error free data set is going to be very fact-specific and subjective.[47] What may be deemed to be complete or error

---

[44] Proposed Rules, Art. 14(4).
[45] Spillner, Test Management.
[46] *See* Theophano Mitsa, *How Do You Know You Have Enough Training Data*, Towards Data Science (Apr. 2019).
[47] *See* Uthayasankar Sivarajah, *Critical analysis of Big Data challenges and analytical methods*, 70 J. Bus. Research 263, at pp. 269-273 ("… the heterogeneity, ubiquity, and dynamic nature of the different data generation resources and devices, and the enormous scale of data itself, make determining, retrieving, processing, integrating, and

free for one facet of society, and one objective of the AI product or system, may not be so for other facets or objectives. Thus, using an absolute standard like "complete and error free" would lead to endless debates over whether the data set truly meets those aspirational goals.[48]

Use of the adjectives "complete" and "error free" in the rule stands in contrast to the use of the adjectives "relevant" and "representative," which suggest a more measured, context-specific approach.[49] This latter approach is the better of the two, and it reflects a reasonable standard for ensuring data sets reflect the community of interest the AI product or system will be serving.

Finally, under the current proposal, regulators have unnecessarily broad authority. They would have the authority to direct companies to remove AI from the marketplace, even if the AI is compliant, and would have access to source code and training data.[50] This raises real concerns with security risks, as well as the sharing of intellectual property and personal and sensitive data. For example, federated learning models use a machine learning technique that trains an algorithm across multiple decentralized edge devices holding local data samples, without exchanging the data samples. The training sets are behind "privacy and security" walls – by design. Beyond privacy, the machine learning developer may not have the right to disclose such data – or even the ability to pull the data – and the Proposed Rules should not undermine these concepts. It is also unclear how regulators expect AI providers to capture and share proprietary information from vendors.

To remedy these concerns, the Commission should revise these principles and adopt more measured standards that allow for the use of diverse data sets in context-specific circumstances, while still retaining principles of representation and relevance. This approach will yield longer term progress toward the goal of reducing potential disparate impact due to bias, while still leaving systems developers and users the necessary flexibility to adopt context-specific, relevant data necessary to serve their objective. Specifically, the Commission should take the following discrete steps:

1. Leverage Industry Standards and Best Practices

First, the Commission should leverage existing industry standards and practices to achieve the goal of more relevant and representative data. Various industry and association leaders have developed data governance standards and best practices which should be the foundation for achieving these goals.[51] In addition, rather than imposing specific requirements

---

inferring the physical world data (e.g., environmental data, business data, medical data, surveil-lance data) a challenging task.").

[48] Even if this standard could be satisfied, simply achieving "error free" and "complete" data sets would not necessarily eliminate all forms of adverse bias because that problem can arise at various stages of model development, training, and deployment is not solely a data training issue.

[49] However, the Commission should provide clarity on what constitutes "sufficient" representation. The answer will likely vary based on different use cases and applications.

[50] *See* Proposed Rules, Art. 64(2), Art. 70(1)(a); *see also*, Explanatory Memorandum, sec. 3.5, p. 11.

[51] *See, e.g.*, National Science Foundation, Dissemination and Sharing of Research Results – NSF Data Management Plan Requirements, Guidance on Data Management Plans (2018); White House Office of Science and Technology Policy, Expanding Public Access to the Results of Federally Funded Research (2013) (directing federal agencies with significant research funding to develop a plan to expand public access, requiring development of data management plans describing long-term preservation of, and access to, data in digital formats); Sherif Sakr and

or standards on training data, the Commission should consider adopting certain model testing and standards and performance when using benchmark datasets. This approach would ensure that the outputs are within an acceptable range, since it is the model output that ultimately determines the real-world impact of an AI product or system.

2. In the Alternative, Clarify Duties Under Art. 10(3)

Second, absent the use of industry governance standards and the use of benchmark datasets, the Commission should clarify the duties under Article 10(3), which articulates a policy for error free data sets. Specifically, the word "shall" in Article 10(3) should be replaced with the word "should," because the notion of securing an "error free" dataset is not realistic. Further, the duty to use "complete" data sets fails to recognize that leading developers use pre-trained data models, which may not be "complete" within the scope of the term used by the Commission. However, excluding the use of pre-trained data models would potentially hinder the development of numerous AI systems. It is therefore critical for the Commission to clarify these duties.

B. Consistency with Other EU Legislation

The Proposed Rules recognize that *existing* EU legislation establishes significant obligations on certain products and systems that are subject to safety legislation in their own right.[52] Examples include cybersecurity systems, transportation systems and aviation systems. These existing safety regimes are comprehensive and far-reaching, and they stand on their own to ensure compliance in the respective area of regulation.

When an AI product or system is developed to serve as an integrated component of such other sectoral system, then it should not be subject to additional, potentially duplicative review or conformity assessments. Subjecting such systems to two separate reviews is inefficient, unnecessary and costly for the party placing such system into the market. Where an existing review process is in place and works to identify potential harms, it is sufficient to rely on that process for any system that may have an integrated AI component.

In these circumstances the Commission should specifically exempt AI products or systems integrated into other regulated systems from any of the obligations of Title III, Chapters 2-3 and 5. Doing so will not increase any risks to EU residents. At the same time, it will ensure that the Proposed Rules are properly harmonized across industry sectors to eliminate potentially costly and duplicative obligations that are not necessary to ensure safety. CTA recognizes that Annex III, which refers to the stand-alone, high-risk AI systems in various sectors, contemplates such a sectoral approach for AI systems that serve as safety components of products, or are embedded in products, that are already subject to third-party assessment.[53] CTA supports this approach based on sectoral legislation and a compliance model that allows requirements for AI systems to be developed at the UNECE level.

Amal Elgammal, Towards a Comprehensive Data Analytics Framework for Smart Healthcare Services, 4 Big Data Research 44 (2016).

[52] *See* Proposed Rules, Title III, Art. 40; *see also*, Recital (63), p. 32.

[53] Proposed Rules, Annex III.

C. Human Oversight

Article 14 sets forth detailed requirements for human oversight of all high-risk AI products or systems. Specifically, this provision requires that all "high-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use."[54]

CTA acknowledges the need for human oversight of certain high-risk AI products or systems in certain situations. Examples include algorithms that predict criminal recidivism, child abuse or neglect, or are used in hiring software.[55] However, the duties of Article 14, as written, are overbroad and should be modified to exclude certain circumstances where human oversight is neither necessary nor appropriate. Although this specific obligation is not necessary for all forms of AI deployed on the market, the Commission should carefully consider, and define, the necessary role and extent of human oversight in this context. Such obligations must be practical and appropriate, and only mandated when absolutely necessary.

For example, human oversight is not feasible in certain autonomous systems, such as fully autonomous vehicles, factory production equipment, or cybersecurity systems where autonomous decision-making in real time is critical to the application. These systems operate in complex environments, interpreting and processing data from multiple sources, which is necessary to make decisions or take actions in an instantaneous fashion.

Consider cybersecurity systems in this context. These are systems that are constantly receiving, reviewing, and acting upon dynamic network and security threats and anomalies, often very rapidly. But if the Commission's proposal would require that humans intervene in every action of such a system its utility and efficacy would be dramatically lower. Human beings are not able to process vast amounts of data and make instantaneous decisions, as some cybersecurity systems do, so imposing human intervention in that process would be counterproductive. Given the growing threat of cybersecurity threat across the world, from bad actors to rogue nations, any limitation or impediment to deploying cybersecurity defenses would have potentially catastrophic affect.

For these reasons the Commission should modify this proposal in several ways. First, the Commission should clarify that the obligation to establish a system of human oversight differs from human intervention. Oversight is appropriate and useful in general, to ensure that these systems are operating in the intended manner and without harming individuals. Oversight involves a pre- and –post system output review to evaluate performance and outcomes but may not involve intervention. Intervention would require human beings to take specific action at certain points in the process to either validate or reject an AI product or system's decision, recommendation or action. As explained above, this is not feasible in certain situations.

Another step the Commission can take is to amend Article 14 to ensure that the obligation only applies in those contexts where human oversight would not materially reduce the

[54] Art. 14(1).
[55] *See* Ben Green and Amba Kak, *The False Comfort of Human Oversight as an Antidote to AI Harm*, Slate (Jun. 2021).

efficacy of the system, or is simply not appropriate given the context of the system at issue (e.g., cybersecurity systems).

D. Distinguishing Roles and Responsibilities of AI Value Chain Actors

The Commission clearly understands the complex supply chain that supports and enables the emerging AI market. Indeed, in its recitals to the Proposed Rules, the Commission acknowledges the complexity of the artificial intelligence value chain.[56] This value chain, which is critical to the continued growth and emergence of robust, reliable and trustworthy AI, includes numerous third parties, many of whom supply software, software tools and components, data sets (both structured and unstructured), cloud storage and related tools, pre-trained models and systems, and providers of network services.[57] This diverse and varied value chain is one indication of the many opportunities presented by this emerging technology, and it reflects real contributions and initiatives of numerous companies.

The Commission should undertake further work to clarify and confirm that these entities in the value chain are not ultimately responsible for the product or service that is put into the market. Without such clarity these innovative and entrepreneurial value chain actors will face potential liability, risk and uncertainty in the future. These organizations will always be asking whether the products and systems placed on the market for which they have provided inputs will not meet the Commission's new standards and, if not, whether the Commission will reach back in the value chain and impose fines, penalties or other liability upon these supply chain providers. Such uncertainty is not consistent with the Commission's objectives here, which include establishing a regime that provides legal certainty to market actors.[58] It also would be a mistake, and contrary to accepted liability standards in place today.

For example, in the case of an automated driving systems, a fully autonomous AI "driver" may be developed by a supply chain provider for purchase by an automotive manufacturer. In the event of a malfunction of that AI system, the causal connection may be too far removed from the original programmer's nexus of control to attribute responsibility in that direction. Rather, at least in the United States, it may be the case that, absent a defect prior to integration, an integrated component into an ultimately defective product falls upon the integrator or service provider using the product or system, not the originating supply chain provider.[59] Further, when communications networks fail (sometimes due to faulty equipment in the network), regulators look to the service provider, not the equipment manufacturer, to remedy any harm to customers. This approach increases accountability and compliance because it focuses the duties and responsibilities of compliance on the service provider who has the commercial or contractual relationship with the end user customer. While contractual commitments between supply chain providers and the ultimate service provider may reallocate risks and responsibilities, the regulatory authorities will consistently look to the "ultimate" service provider for compliance with appropriate rules. The Commission should clarify the same approach here and clarify that the supply chain service providers are not liable for failures of any AI product or system that may result in fines, penalties or other liability. Only those entities that

[56] Proposed Rules at Recital (60), at p. 32.
[57] *See* Hau Lee *et al*., White Paper: Value Chain Innovation: The Promise of AI, Stanford Graduate School of Business (2018).
[58] Proposed Rules, Recital (6) ("The notion of AI system should be clearly defined to ensure legal certainty…").
[59] *See* Herbert Zech, *Liability for AI: public policy considerations*, ERA Forum (2021).

"place into the market"[60] or "put into service"[61] AI products or systems should be subject to potential liability.

E. Clarify Carve-out of AI Systems That Are Safety Components Within the Scope of Other Acts

Certain components of the Proposed Rules appear to be in conflict and should be modified to eliminate conflict or ambiguity around the scope or application of any final rules. For example, Article 2(2) provides a carve-out for AI systems that are safety components of products or systems, or which are themselves products or systems and already covered by existing EC regulations or directives (as listed therein). However, Art. 6(1) (of Title III) appears to contradict the plain language of Art. 2(2) and appears to pull these very systems into the scope of high-risk AI systems subject to the requirements under Title III.

Article 2(2) clearly excepts certain systems that are already covered by existing law: "[f]or high-risk AI systems that are safety components of products or systems, or which are themselves products or systems, falling within the scope of the following acts, only Article 84 of this Regulation shall apply: …"[62] (and citing numerous EC regulations that establish comprehensive liability schemes). The rationale here is obvious. If existing legal regimes already guard against potential harm, there is no need for additional duplicative regimes to guard against the same potential harm.

The wisdom of this approach is, however, undermined by seemingly contradictory language in Article 6(1). Here the Commission states that:

> "Irrespective of whether an AI system is placed on the market or put into service independently from the products referred to in points (a) and (b), that AI system shall be considered high-risk where both of the following conditions are fulfilled:
>
> (a) the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II;
>
> (b) the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II."[63]

The concern here is that Article 6(1) may close the exception explicitly provided in Article 2(2). On its face, the language of Article 6(1) broadly categorizes all AI systems such that when the system is used as a safety component or product covered by the Union harmonisation legislation, it is required to undergo a third-party conformity assessment pursuant to specific Union legislation. Thus, in broad strokes, the language of this article seems to

[60] *Id.* at Recital (5).
[61] *Id.*
[62] Art. 2(2).
[63] Art. 6(1).

classify nearly all AI systems and classify such systems as high-risk, regardless of whether they are already subject to current requirements under existing law.

The Commission should take this opportunity to clarify and confirm that AI products or systems that are safety components already governed by other regulations are not subject to the requirements of the Regulations. If necessary, existing regimes may need to be updated to reflect new technology.

F. Recordkeeping and Reporting Requirements

1. Recordkeeping

Article 12 of the Proposed Rules sets forth detailed and comprehensive recordkeeping obligations of covered providers. Specifically, these include:

- A duty to create event logs capable of enabling the automatic recording of events while the high-risk AI product or system is operating;
- Logging capabilities at a level of traceability that is appropriate to the intended purpose of the system (throughout its lifecycle);
- Logging capabilities shall also "enable the monitoring of the operation of the high-risk AI system with respect to the occurrence of situations that may result in the AI system presenting a risk within the meaning of Article 65(1) or lead to a substantial modification, and facilitate the post-market monitoring referred to in Article 61";
- Additional logging capabilities apply to AI systems referred to in paragraph 1(a) of Annex III, which include:
    - recording of the period of each use of the system (start date and time and end date and time of each use);
    - the reference database against which input data has been checked by the system;
    - the input data for which the search has led to a match;
    - the identification of the natural persons involved in the verification of these results, as referred to in Article 14(5).

The proposed logging and recordkeeping duties laid out above are quite substantial and will likely require significant investment from AI product or system providers to develop and maintain such capabilities. This proposal amounts to a duty to undertake a historization process for all data and models, which would be a momentous undertaking.

To comply with these requirements, AI products or systems providers will be required to undertake significant work to build into these systems the logging capabilities outlined above. Further, these logging capabilities must be capable of delivering "traceability that is appropriate to the intended purpose of the system (throughout its lifecycle); …" and enable monitoring "with respect to the occurrence of situations that may result in the AI system presenting a risk …" within the meaning of certain articles under the Proposed Rules. Putting aside the ambiguity presented by these vague standards, it is clear that complying with these extensive requirements will be expensive and burdensome to maintain, especially for SMEs operating on narrow margins and with fewer resources. That, in turn, will lead to decreased investment in core

products and services, will undermine innovative small companies from entering the market, and reduce competition in the market.

But the burdens associated with this proposal need not be overwhelming if the Commission chooses to cap the period of time for which such logs and records must be maintained. A sensible limitation of time is three years, which will provide regulators sufficient time to look back to review historical records, but is less burdensome to AI products or systems providers who will only have to retain such information for a limited period of time.

2. Reporting

The Proposed Rules would also mandate certain incident reporting obligations. But the current proposal is vague and ambiguous. Absent clarification from the Commission (and significant narrowing of the reporting obligations), there is a real risk that the rule will lead to significant uncertainty in the market and potential over-reporting of incidents that do not present material harms and which may simply burden Commission and EU staff responsible for reviewing and responding to such reports.

As currently drafted, the rule requires providers of high-risk AI systems placed on the EU market to report "any serious incident" or "any malfunctioning" of these systems that constitutes a breach of obligations under EU law intended to protect fundamental rights. Framed this way, providers will be forced to first asses what constitutes a "serious" incident or any malfunctioning of the system, and second whether these events have led to a breach of obligations under EU law to protect fundamental rights. Thus, providers will be forced to make subjective decisions about the level of severity of an incident, whether a system has malfunctioned (in any way) and whether laws protecting fundamental rights have been breached. All of these criteria are broad, open-ended triggers that will vary significantly based upon the facts of any particular circumstance. Further, they will undoubtedly lead to significant range of self-reported events, some serious and worth the Commission/EU staff's time, and many others not.

Further, the reporting proposal fails to account for the fact that there may be multiple algorithms that are used in a model or AI system, and the proposed rule does not acknowledge this fact or explain whether these reports are due on an algorithm, model or system basis. The Commission should clarify this point. Similarly, the Commission should clarify that conformity assessments are not required on a per model basis, but are required only of an entire AI product or system.

V. CONCLUSION

CTA and its members have a significant interest in ensuring that European consumers benefit from AI-powered products and services. The Commission should proceed carefully to ensure that its policies promote continued development and deployment of AI products or systems that enhance the lives, safety and interests of European consumers. CTA stands ready to continue its central roles in the development of consensus-based standards that advance these goals and promotion of policies supporting continued dynamic growth and innovation throughout the consumer technology industry.

/s/ Douglas K. Johnson
Douglas K. Johnson
Vice President, Emerging Technology

/s/ Michael Petricone
Michael Petricone
Sr. Vice President, Government and Regulatory Affairs

Dated: August 5, 2021