Increasing the effectiveness of the EU's AI regulation by smart inclusion of the AI value chain

Introduction

This short paper expands on the role of the value chain in the development and deployment of AI systems on the EU's Internal Market. The paper describes the need for, and then specifies a framework that enables AI value chain actors to provide assurance of compliance to other actors, including providers and users, in a cost-effective manner.

The *Whereas* (60) clause of the draft AI regulations acknowledges the complexity of the AI value chain, and recommends that actors in the value chain should cooperate, as appropriate, with providers and users to enable the compliance of their AI systems with the obligations under this regulation. Although still relatively immature, AI value chains are indeed increasingly complex. They will undoubtedly evolve over time as AI becomes pervasive across all sectors of business, the public sector and society more generally.

The draft regulation defines an AI provider as an entity "..placing it on the market or putting it into service under its own name.." Some providers will be technology companies with experience of managing an AI value chain. Providers in other sectors ranging for example from health care providers to transport operators, may not have that experience. Given the diverse obligations of the various actors in Titles III and IV of the draft AI regulations, it is clear that all providers would, regardless of their experience, benefit from a framework that provides a standardised trusted assurance mechanism that evidenced compliance throughout the value chain. Actors in the value chain would benefit from lower compliance costs, reduced risk and be less at risk from the disadvantage of information asymmetry. Without a common framework different providers might take different approaches, leading to multiple incompatible and fragmented procurement or compliance verification protocols with increased compliance costs and increased risk.

This paper describes the requirements and desirable attributes of such a framework. The framework must provide a practical approach that optimises the way in which actors in these evolving AI value chains can meet their contractual and other obligations. These are obligations that AI providers will inevitably impose upon them in order that AI providers in turn can be confident they can meet the requirements of the EU's proposed AI regulation.

The AI value chain explained

AI systems are built through complex value chains like many complex industrial or automotive products. Unlike industrial products, however, AI systems' value chains rely significantly on non-contractual relationships (e.g., open-source libraries, datasets, pre-trained models, model architectures, etc.) and "problem-solving"-based scope of work that evolves over time as new aspects of the problems are discovered.

Multiple companies and entities can be actors engaged in the building and deployment of an AI system, including dataset providers, cloud providers, chipset providers, algorithm developers, and others. Some actors can validate compliance with certain obligations while compliance with other obligations can only be provided from elsewhere in the value chain. For example data governance

requirements (Article 10) will be under the effective control of the dataset provider or the test data provider.

A framework has value beyond meeting regulatory requirements – it can build trust

Most AI systems will be categorised as low-risk, for which no additional regulatory requirements are proposed. Yet we know that AI will remain under public scrutiny beyond regulatory obligations. For low-risk AI systems, there are already many different company-specific codes of conducts and ethical guidelines. However, these do not foster contractual trust or ease the compliance burden among value chain actors.There is a need for a framework that would complement and simplify the contractual landscape, benefitting all actors and particularly actors who are European SMEs facing an uncertain but increased compliance requirement.

Consistent with harmonized standards

The framework should be industry-led and developed in a manner that is consistent with the standards being developed by CEN/CENELEC and other global standards bodies. The framework must be more than a standard and include practical advice and guidance that makes compliance for large and small organizations easier and less costly. It should also be developed and made available more quickly than harmonized standards.

The framework could also serve as the foundation for future-proof European liability rules

A structured exchange of technical information between the different actors in the value chain will be the foundation of an efficient and transparent distribution of liability. A particular liability-sharing mechanism for the supply side and specific to the AI-related industry is needed to support the enforcement of this modernised liability framework. In order to help prevent damages, this disclosure of technical information should occur by default rather than only after damage occurs, in the hope that the operators could make more informed decisions about the operation of the product.

A self-regulation contractual framework for conformance

We propose that industry develops a governance framework that would address the issues highlighted above. This framework should rely on cost-effective protocols so that actors in the value chain can assure each other of compliance with the AI regulations. The objectives of this framework are to

- Ensure verifiable trust among the value chain actors.
- Ensure cost-effective compliance by all actors involved in “providing” the AI system.
- Minimize transaction costs within the industry globally.

The framework should be a one-stop, standardized solution to cost-effectively satisfy regulators’ requirements and enhance customers’ trust while minimizing suppliers’ burdens. A broad representative group of suppliers should drive the development to ensure the framework caters for the many different types of value chain from eg open source software models to traditional hardware supply chains.

Specifically, the framework should satisfy the following requirements:

- For each AI system, each actor involved in the supply chain would prepare and provide a standardized, encrypted and immutable “assurance file” and share it with the next “node” in the production network.

  - ❑ Filling this assurance file requires preforming the legal and technical tests relevant for compliance with regulations and enabling trust.

  - ❑ The template file would be “role-specific”; e.g. the identified dataset provider would fill a document on conformance tests relevant to data, the algorithm provider would fill a document on conformance tests relevant to algorithms, and so on.

- The assurance files capture answers to a series of relevant questions and also provide technical evidence of compliance with regulatory requirements (including requirements and tests as set out in harmonized standards).

- The files “travel” through the value chain as the AI system is developed and are ultimately compiled at the customer-facing node.

- The framework would form a step-by-step fulfillment of the various requirements imposed by regulators and ensure transparency along the value chain. Consideration should be given as to how the data in these files could be easily machine readable to facilitate future automation.

The framework must be adaptable over time, and help industrial procurement systems to converge on common requirements. The framework would be mutually beneficial in the following sense:

- As a supplier, this helps ensure that the responsibility for compliance is fulfilled regardless of what the customers uses the AI system for.

- As a customer, this ensures you can trust the suppliers and the rest of the supply chain and have contractually fulfilled your due diligence.

These files would be standardised to ensure modularity of the value chain: knowing the framework’s protocol enables you to coordinate with all others in the industry, rather than having to tailor documentation to each customer’s specific protocal or approach.

Our recommendation

We propose that industry develops a framework along the lines set out above designed to facilitate industry-wide compliance with the AI regulations.

In the context of high-risk AI systems, the framework would

- Help collect relevant documentation throughout the value chain for compliance with regulatory obligations such as risk management, data and data governance, technical documentation, record-keeping, information provision, quality management systems, conformity assessment, registration, etc.

- Ensure the right technical tests and legal tests are carried out by suppliers, and enable the required transparency between business partners in order for all value chain actors to have equivalent levels of information.

In the context of compliance for low risk AI systems, the framework would

- Help translate company-specific codes of conduct for low-risk AI systems into something tangible, standardised and usable by suppliers and customers.

- Where transparency requirements apply, ensure all actors have equivalent levels of information (e.g. system integrators' automatic disclaimers solutions, deployers, custom-made notifications panel, etc.)

The framework would help cost-effectively satisfy post-market surveillance authorities requests as well as strengthen conformity assessments (whether 3rd party or self-performed). It would also help actors be more confident that other actors involved in the value chain are fulfilling their regulatory obligations. By providing a one-stop solution, it would help ensure a coherent self-enforcement mechanism to be adopted alongside official harmonized standards, reducing compliance costs significantly.

About Global Digital Foundation

Global Digital Foundation is a platform for dialogue between policymakers, stakeholders and scholars in support of evidence-based policy for the digital society. It is also a source of briefings for all who have a personal or professional interest in policy that affects the development and use of digital technology.

www.globaldigitalfoundation.org paul.macdonnell@globaldigitalfoundation.org

5th August 2021