Huawei's input to DG CNECT Inception Impact Assessment on AI

Huawei started as a small company in China and we have grown to be a world leader in digital technologies. We have been a trusted partner in Europe for 20 years and we are committed to staying in Europe. Today, we employ over 13000 people in Europe, running two regional offices and more than 20 research sites. Huawei is a world leader of digital technologies working with European industry partners to support a diverse ecosystem of full-stack, all-scenario AI offerings. For example, Huawei MindSpore AI framework, Huawei Ascend AI microprocessors, Huawei contributions to open source hardware and software for AI and cloud computing communities, Huawei Harmony IoT operating systems, and mobile services for navigation and search.

Following the fast deployment of AI applications and use cases in different sectors of the economy, we believe that now is the right moment to further expand the discussion about the product safety and liability aspects of AI technology. We need to ensure consumer protection and a robust regulatory framework which should remain technology neutral. High-risk applications should be regulated under a clear legal framework which provides on the one hand a legal certainty for enterprises and on the other hand adequate protection for citizens.

There is a need for a better definition of high-risk applications because it is complex to understand and explain Artificial Intelligence under one fixed definition without the context of different use cases and applications. There is also a need to build trust in AI through awareness and promotion of digital skills and AI knowledge by incorporating new ways to learn AI and ICTs in primary and higher education curricula and by providing EU-wide free data, statistics, and AI courses for all (adults and children).This would help citizens to better recognise different aspects of AI technologies and promote the uptake of AI.

We believe that AI will be used in almost every sector of the economy, however we still need to observe the technology until it gets mature. Complexity, opacity and autonomy are variable terms when it comes to the definition of AI. There is no clear delineation between software and AI. Regarding the definition of AI we propose that:

- AI application risk assessments should focus on intended use of the application and the type of impact from the AI function;
- Detailed assessment lists and procedures must enable self-assessment to reduce the cost of initial risk assessment; and
- Assessment lists and procedures should match sector-specific requirements.

The existing legal framework based on fault-based and contractual liability is sufficient for the state-of-the-art including AI so extra regulation is unnecessary, would be over-burdensome and discourage the adoption of AI.

The risk assessment must take an application-inclusive approach involving not only the properties of the algorithms and training data but also aspects such as the reliability of

HUAWEI

sensors/data sources and user interfaces, which can significantly impact application performance in real-world use.

For the assessment of high-risk AI applications, a bottom-up approach may be more effective, where industry should play an important role in finding and establishing clear assessing criteria, and providing practical assessment guidance. There is a need to bring together consumer organisations, academia, member states or businesses to assess whether an AI system may qualify as high-risk. The Commission and the standing Technical Committee high risk systems (TCRAI) could assess and evaluate an AI system against high-risk criteria both legally and technically.

A voluntary labelling system could complement the requirements for high-risk applications. In the complex supply chain of an AI system with multiple stakeholders, these labels should be designed for different roles based on their technical specifications and aligned with specific sectors, since a 'one-size-fit-all' scheme may be ineffective. A governance model that considers the supply chain should develop the right criteria and target the intended goal of transparency for consumers/businesses, and incentivize responsible AI development and deployment.

As regards the quality of training data sets, it is indisputable that any AI use case will benefit from high quality and representative data sets. However, there is an element of subjectivity involved in defining what high quality may mean for a particular use case. Setting a fixed standard may unnecessarily constrain the work of data scientists.

Huawei further refers to our response to the AI Whitepaper consultation in the ANNEX below where we elaborated on these aspects in more detail.

ANNEX

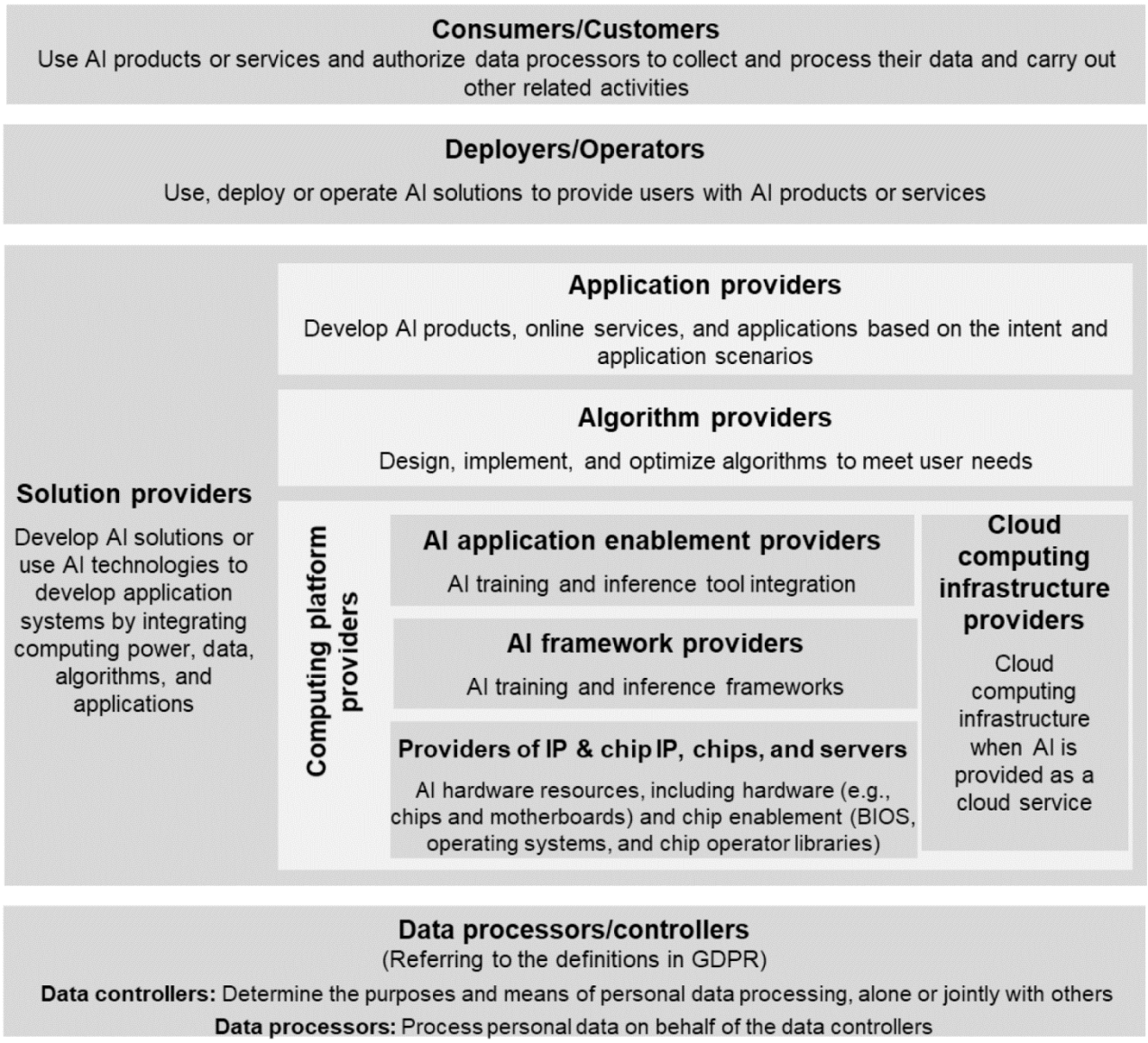
Huawei's Response to the European Commission's Whitepaper on Artificial Intelligence

On the Ecosystem of Trust

A. Establishment of a multi-actor governance framework

The AI chain is complex with multiple market participants providing different component such as chips, sensors, datasets and software. As the typical activities and technical specifications involved are different for each role, a "one-size-fit-all" approach cannot meet the requirements for all of the participants. For example, data controllers need to consider how to disclose the source, usage, and measures for handling datasets, while algorithm and application providers should mainly consider how to provide objective and easy-to-understand explanations for their algorithmic models. In order to provide clear guidance for different actors, it's necessary to identify the typical activities and requirements for each role.

Such a multi-actor framework may be defined as followed:



Collaboration of diverse market participants would form a dynamic ecosystem and facilitate innovation along the value chain, but also makes the whole system more complex and hard to regulate. If an AI system takes undesirable actions, it may be difficult to identify the source of the problems and hold the most relevant actors accountable. By establishing a multi-actor governance framework and reducing vulnerabilities of each parts, the robustness, security and quality of the AI system could be enhanced.

Each participant should focus on different measures when they provide AI components at different layers. There are some recommendations for the typical roles:

1. Data processors/controllers: Ensure data management and other related operations fully comply with General Data Protection Regulation (GDPR) and other applicable laws and regulations.

2. AI computing platform providers:

- Information security hardening for hardware;

- Defence mechanisms for machine learning;

- Trustworthy implementation of operators;

- Secure and robust operation environment for AI frameworks and AI application enablement;

- Traceability, privacy protection, security, and robustness of software.

3. AI algorithm providers: Research and develop algorithms that meet a certain standard of security and robustness, and use statistical analysis, semantic verification, and other methods to continue enhancing the capabilities of algorithm programs to run as expected.

4. AI application providers: Provide services, applications, sub-systems, and supporting O&M mechanisms that meet trustworthiness requirements in the domain by using AI algorithms and computing platforms, like the cloud, edge, and devices, that meet certain security standards.

5. Solution providers: Ensure AI systems meet industry-specific needs and are trustworthy, and provide solutions and supporting services that meet the safety and ethical requirements of each scenario. This can be achieved through various methods, such as pre-event analysis, in-event intervention, and post-event audit and evaluation.

6. Deployers/Operators: Perform acceptance tests to determine whether AI systems can fulfil their intended purposes, and help identify potential harmful outcomes and make appropriate corrections to ensure that the deployment goals are achieved. Effectively control and prevent risks related to AI security and privacy during deployment and operations.

7. Consumers/Customers: They have the right to choose whether to use AI systems. If they use AI systems, they must follow product/service instructions to ensure products or services are used safely. Avoid using AI systems for purposes that violate laws or ethical rules, such as developing intentionally misleading photos or video and audio content.

Such a multi-actor framework would help further refine and divide AI governance architecture at a nuance level. This will help practitioners identify emerging risks related to different components, and proactively take measures to prevent these risks. In addition, such a multi-actor framework would help increase the traceability of different layers of AI systems and determine the scope of responsibility of each layer. For example, we can use technical means such as data security labelling (i.e. labelling data security, identifying data tampering, and finding the cause), model signature tracing, and model watermarks to help determine the source of data tampering or leakage, or the root cause of a security failure.

It's essential to work with standards organizations to further codify the best practices of AI governance into global standards and specifications. Also, the close public-private partnerships could help effectively collect best practices of AI governance and provide minimum acceptable standards for different layers.

B. Regulatory framework of high-risk AI applications

We strongly support the fundamental concept of basing regulatory requirements for AI application on an assessment of the degree of risk posed by an AI application. We agree with the approach to determine "high-risk" AI applications considering both the sectors and the use, and would like to know about the concrete definition and a list of specific "high-risk" applications at a granular level, which would bring legal clarity and certainty.

1. Ex ante and ex post requirements

For high risk applications, some ex ante requirements would be desirable. This will depend on the particular use case and context. Generally, requiring the involvement of domain experts would be desirable: for example, with digital healthcare solutions, an ex-ante conformity assessment should involve the expertise of doctors and nurses.

Ex ante requirements can also be helpful to companies as the legal certainty allows them to absorb costs in advance and tailor products or solutions accordingly. After a solution is given the green light, the relevant regulator will need to monitor compliance (for example and if appropriate, through regular checks, as the FCA might do with financial products), but also determine whether the original requirements were adequate. If not, these could be modified and/or an ex post requirement might be added. Regulators should ensure that imposing any additional action is subject to a thorough cost-benefit analysis.

Meanwhile, we believe the majority of machine learning applications should not be deemed high risk and so should not be constrained by ex-ante requirements. In this case, we expect ex post market surveillance to be sufficient and innovation-friendly, provided regulators and national authorities are adequately trained.

2. Institutional framework

Legislation alone cannot guarantee a safe and secure environment for citizens without adequate regulatory oversight to enforce it. The foundation for ensuring that AI is trustworthy and secure is to ensure national regulators are sufficiently resourced (in terms of talent, training, and tools) to be able to scrutinize AI-related risks in their respective verticals.

Ensuring regulators from different Member States are connected to one another is another important requirement: the focus should be on consistency mechanisms and the harmonization of decisions and requirements from the member states' competent authorities, as well as the relevant institutional coordinating within EU. Guaranteeing this from the start will ensure future regulatory frameworks will not suffer from the shortcomings such as those highlighted in DigitalEurope's response to the DG JUST Roadmap Consultation on GDPR.

3. Conformity assessment

We would propose that a clear definition of "high risk" scenarios should be provided and reviewed regularly with transparent process and should be applied to all vendors.

Regarding the process and criteria for assessing the risk level of an AI application, we acknowledge the intent behind the cumulative sectoral + intended use approach, but consider the reliance on allocation of "high-risk sectors" to be extremely difficult to meaningfully implement in practice, as indicated by the examples of "exceptional instances" that were already given in the AI white paper. This problem is further complicated by the difficulty of establishing a useful application independent definition of AI. As an alternative, we would propose:

- AI application risk assessments that focus on intended use of the application and the type of impact the AI function has. E.g. does the intended use involve potential long term consequences? Doe the AI determine the output of the application in a way that makes it difficult for humans to assess if the outcome is correct?

The risk assessment has to take an application inclusive approach involving not only the properties of the algorithms and training data but also aspects such as the reliability of sensors/data sources and user interfaces etc., which can significantly impact application performance in real-world use.

- Some compliance requirements are based on subjective judgments, e.g. practitioners and users have different understanding and requirements on Explainability issues, where an external conformity assessment procedure operated by third parties is more professional and reliable.

- Reduce the cost of initial risk assessment by providing detailed assessment lists and procedures to enable preliminary self-assessment by the industry.

- Acknowledge sector specific requirements by providing/modifying the assessment lists and procedures to match sector demands.

- The risk assessment lists/procedures should be co-developed with multi-stakeholder input including Standards Development Organizations, and will need to be periodically revised.

- Beyond application specific factors, the risk assessment may also need to take into account additional factors such as: anticipated number of users, especially if the risk is to society as in the case of news recommender systems; dependence on support infrastructure, e.g. patient embedded medical devices that will fail if the specialized service provider for the cloud based AI ceases operating

C. Voluntary labelling scheme

Labelling seeks to address concerns that regulation doesn't reach, it can help to strike the right balance between protecting users and encouraging innovations. A labelling scheme can provides transparency with information that can be easily understood and assessed by users and other stakeholders, and help to increase trust.

For this purpose we would propose that a labelling scheme with clear specification should be provided through public and private partnership. An industry-led approach would be effective, where industrial associations with the technological and industrial know-how could be encouraged to explore in voluntary labelling frameworks within different scenarios, and provide best practices and guidance for different applications.

D. International collaboration

Since the digital economy driven by AI typically involves an international value chain, a fragmented governance framework may lead to regulatory arbitrage and vicious competition across different regions. Establishment of a multilateral AI governance mechanism consisting of members from governments, civil society and private-sector would be essential to promote a basic consensus of trusted AI across the world and avoid fragmentation of responsibilities globally.

We may learn from the practical experience of such multilateral governance mechanisms in the ICT industry, especially the success story of the 3rd Generation Partnership Project (3GPP). Although the nature of telecommunications technology is different from AI, it could be worthwhile analyzing the multilateral collaboration mechanism formed in the ICT industry, as part of the efforts to drive a world-wide consensus on AI governance frameworks.

The 3GPP is a collaborative project initiated by multiple partners/members to promote the standards development and adoption of emerging telecommunications technologies. Thanks to the open multilateral governance mechanism of the 3GPP, 5G has seen the industry converge on a universal set of standards, avoiding the fragmentation of standards in 2G, 3G, and 4G. The coordination of standards have benefited all stakeholders across the value chain. This will also further incentivize investment in 5G and accelerate commercial deployment.

The success of 3GPP has shown that a multilateral international mechanism could be an effective approach to coordinate the global governance landscape of emerging technologies like AI, where a specialized, permanent international governance organization or a non-permanent international mechanism is essential.

The 3GPP consists of three types of members taking different roles in the collaboration:

- Organizational Partners (OPs) [1] , specifically regional Standards Development Organizations coming from different regions, which are the most important members of 3GPP, working together to determine the general strategy of 3GPP. They authorize the 3GPP to produce Technical Specifications (TS), and then set standards for their own regions based on these TS.

- Market Representation Partners (MRPs), such as GSMA, Next Generation Mobile Network (NGMN) Alliance, 3G Americas, and UMTS Forum. These MRPs offer market advice to the 3GPP and keep the 3GPP informed of the market consensus on requirements for technologies falling under the remit of the 3GPP, so as to contribute to the application and development of mobile communications networks worldwide.

- Individual Members (IMs) who can contribute technically to one or more of the Technical Specification Groups within the 3GPP scope.

Refer to the 3GPP, the multilateral AI governance mechanism may have the following characteristics and functions:

- Consist of standards organizations authorized by regional governments. The AI principles and governance frameworks developed within this mechanism could be recognized and incorporated by governments in different regions.

- Foster public-private partnerships. The private sector should be encouraged to play its role in technology R&D and standards formulation, and foster public-private partnerships to realize well-thought-out AI governance principles.

- Drive the development of international standards. International standards and specifications for AI technologies (e.g. for security and trustworthiness) can be developed through collaboration with standards organizations, with a particular focus on the formulation of acceptable minimum baselines.

- Establish an authorized certified test mechanism. Authorize independent international test organizations to evaluate and test AI products or services based on unified testing specifications to ensure that these products or services meet the requirements for market access.

- Promote the application of technologies. Collect data and advice on market requirements in order to promote the application and development of AI in various industries.

Based on Huawei’s experience of open collaboration in the ICT industry, we are willing to support Europe to lead in establishment of such a multilateral, democratic, open, and transparent international AI governance platform, which would promote collaboration among stakeholders cross the world, and advance the uptake and adoption of AI in a fair manner.

[1] The 3GPP unites seven Organizational Partners from six regions: ETSI from Europe, ATIS from USA, ARIB and TTC from Japan, CCSA from China, TSDSI from India, and TTA from Korea.