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

June 2020

Table of Contents

Introduction

Huawei welcomes the opportunity to take part in the open consultation of the European Commission's White Paper on Artificial Intelligence "A European approach to excellence and trust".

We strongly support EU's focus on both an "ecosystem of excellence" and an "ecosystem of trust". Excellence and trust are closely linked: only an excellent AI system that meets high scientific standards could gain trust from users, while the trust is a crucial factor to promote uptake and adoption of excellent AI applications. From this perspective, it's crucial to keep a balance between development of technologies and regulations of applications.

In light of the above consideration, we would like to propose the following recommendations on both of the ecosystems of excellence and trust.

On the Ecosystem of Excellence

A. Accessible, affordable and green infrastructures

Uptake and adoption of AI technologies in a variety of scenarios are bound to engage more computing infrastructures both at the cloud and the edge levels, steadily increasing the demand for computing power, which is becoming a key bottleneck of the AI adoption process. In order to build accessible and affordable infrastructures for all developers including SMEs and individuals, the policies that **ensure sufficient investments in infrastructures** is a prerequisite.

AI applications requiring a mass of data would also increase demand for higher-quality networks that enable smooth and real-time data traffic. Policy tools and resources to **improve the network infrastructures** would lay a solid foundation for facilitating adoption of AI. Core policies may include: 1) spread out an extensive monitoring matrix to supervise the status of network deployment and 2) leverage private capital to build network infrastructure through Public–Private Partnership (PPP).

The heavy power consumption of typical computing infrastructures like data centres is a major challenge to the climate change issue. It would be beneficial for practitioners if the Commission could **offer guidelines and incentives to deploy energy-conserving and green computing power infrastructure.** From this perspective, we recommend that the Commission could take into account the following actions: 1) advocate industry association to set energy-conservation goals, 2) directly invest in new energy industry, and 3) formulate a carbon emission exchange mechanism and put a high price tag on limited.

B. SMEs and AI uptake

SMEs are the cornerstone of the European economy and their success is vital especially since they employ over 65% of the workforce in Europe. SMEs need to remain competitive in a continuous evolving digital labour market by adopting sophisticated digital technologies like Artificial Intelligence (AI), cloud computing, blockchain technology and others. The Commission and governments need to support SMEs to improve access to technologies like AI by **encouraging synergies between SMEs and big corporations**.

SMEs face the challenges of developing new innovative services in an increasing competitive market. Big Tech companies can assist not only in building up the capabilities of SMEs cloud computing infrastructure, but also help them engage in independent software vendor partnerships and cooperation in order to develop their cloud services.

C. Digital skills, literacy and AI education

Digital technologies like Artificial intelligence offer an excellent opportunity to increase productivity rates and tackle the shortage of skills. The right skills help individuals to adjust to a changing labour market and society in times of technological developments, global and demographic challenges. Digital technologies support the growth of all types of industries. Some data literacy and a basic understanding of how AI works will be essential to build trust and support adoption. By failing to properly equip and upskill European citizens, Europe risks losing its competitiveness. As the Covid-19 crisis and debates around contact tracing apps has shown, the need for digital skills and data literacy is higher than ever. In the light of such developments, we recommend that the Commission:

- **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) – similarly to the Finish 'Elements of AI' course. There is a need for an inclusive, lifelong learning-based and innovation-driven approach to AI education and training, to help people transition between jobs fluidly. The Commission should also provide the necessary tools to safeguard social inclusion, strengthen gender balance and encourage diversity in the labour force.
- **Increase cooperation and coordination between public and private sector**. This is crucial as the upskilling of European workforce can be better achieved by leveraging private sector expertise. The Commission should explore defining competency-based curricula and facilitating placement schemes by encouraging dual degrees, and sector-specific degrees (e.g. machine learning and electrical engineering for manufacturing). The European University is a good initiative in this direction. Conversion courses allowing the workforce to switch to transition between different careers and sectors would also strengthen the flexibility and resilience of the workforce. An example of such an initiative is the UK Government's Office for Artificial Intelligence programme to provide funding for providers to develop postgraduate conversion courses in these areas. The creation of a Europe-wide platform for digital higher education and cooperation between schools, universities, research centres, and employers would be another important step in the right direction. There is an opportunity for Europe to lavage online education courses that have been developed as a response to distance learning requirements under COVID-19 shutdowns.
- **Ensure that well established European tools and frameworks such the new Europass[1] and the European classification of Skills, Competences, Qualifications and Occupations (ESCO)[2] include information on occupations, skills and qualifications related to Artificial Intelligence (AI).** This would improve transparency and portability of AI qualifications and skills between countries and people would have access to information on AI jobs and training opportunities across EU. People

[1] https://ec.europa.eu/futurium/en/europass/new-europass

[2] ESCO (European Skills, Competences, Qualifications and Occupations)

will be also able to identify their skills gaps related to AI and identify the right trainings for them in order to reskill/upskill.

- **Facilitate the issuing and verification of AI credentials in order to enhance interoperability across different national education systems in Europe.** The Europass Digital Credentials[3] project could play an important role for achieving this.
- **Support the regular analysis of skills supply, demand, mismatches and development.** The European Centre for the Development of Vocational Training (CEDEFOP)[4] already plays a crucial role on this by using big data analysis techniques and ESCO to extract information from online job vacancies[5] and inform training providers on how relevant their training programmes are in a continuous evolving labour market. Such information will also enable certain impactful AI use cases, such as the use of machine learning to match job seekers with potential employers.

D. AI for Inclusive growth

AI technologies have great potential for addressing global challenges such as poverty, inequality, climate change, and healthcare. In order to promote the use of AI to attain SDGs, it could be encouraged to establish foundations that **fund AI projects run by NGOs dedicated to improving social and environmental well-being**. Also, it would be effective to work with the private-sector to **launch flagship "AI for Good" programs**, which spreads the idea further.

In addition, it would be beneficial for European policy makers to embrace new technologies and utilize AI to improve public services. **The adoption of AI in the public-sectors** including healthcare, education, transportation, and environmental protection would effectively enhance the efficiency and quality of public services, which would benefit European citizens and promote social well-being. This would also help policy makers to better understand the nature of AI technologies and obtain hands-on experience in AI applications, and thus inform and facilitate future rulemaking.

On the Ecosystem of Trust

A. Establishment of a multi-actor governance framework

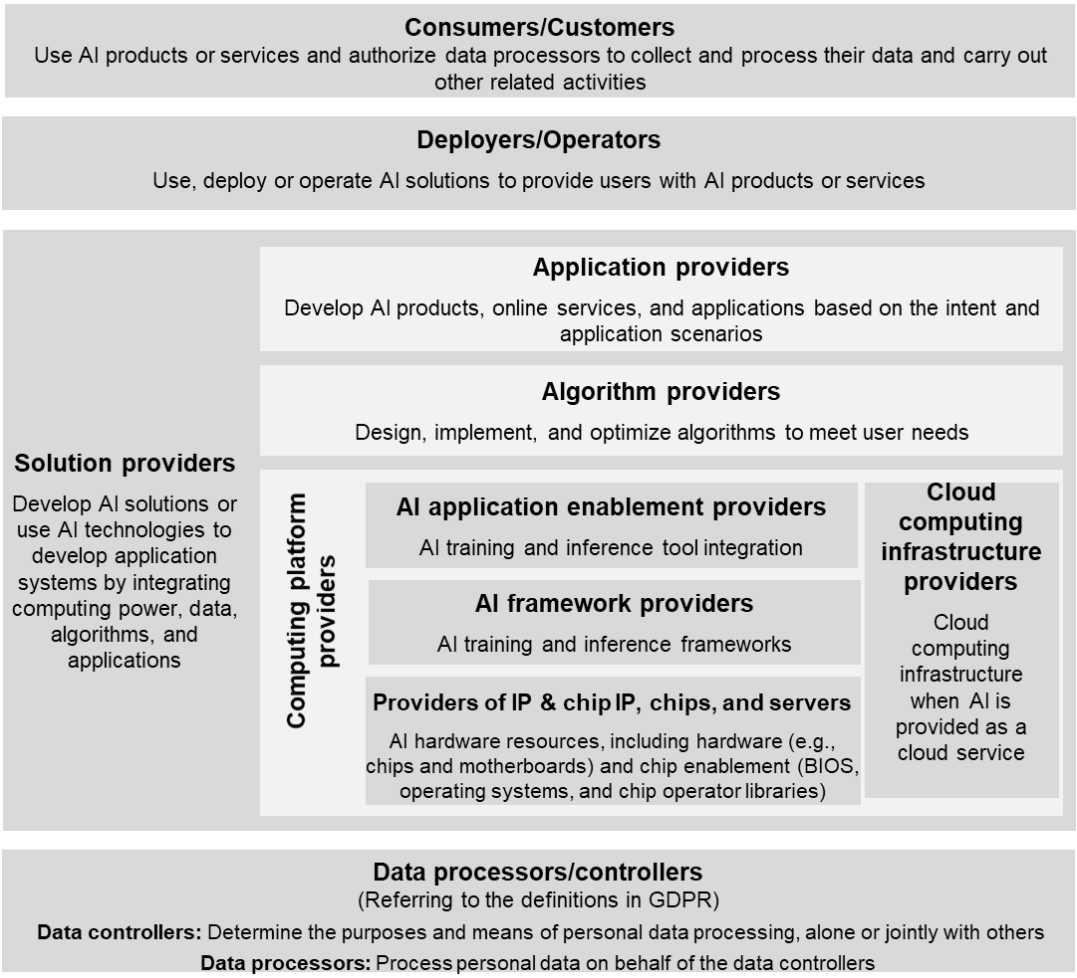
The AI chain is complex with multiple market participants providing different component such as chips, sensors, datasets and software. As the typical activities and technical specifications involved are different for each role, a "one-size-fit-all" approach cannot meet the requirements for all of the 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:

[3] https://ec.europa.eu/futurium/en/europass/digitally-signed-credentials

[4] https://www.cedefop.europa.eu/

[5] More info here



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 harmonisation 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 Organisations, 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 econoAmy 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 analysing 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)[6],** 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.

[6] 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.

- **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.

About Huawei

Founded in 1987, Huawei is a leading global provider of information and communications technology (ICT) infrastructure and smart devices. We are committed to bringing digital to every person, home and organization for a fully connected, intelligent world. We have nearly 194,000 employees, and we operate in more than 170 countries and regions, serving more than three billion people around the world.

Huawei's contribution in Europe

Huawei is committed to Europe. The company sees Europe as its second home base and wants to contribute to **European growth** and towards Europe's **technology leadership** in the world. In Europe, Huawei supports clients' full control of data, offering technical solutions that are efficient, innovative, and trustworthy in terms of data protection, data localization, citizens' privacy, cyber security, and the ethical considerations of the applications and equipment used on European soil. Through open collaboration with ecosystem partners, Huawei creates lasting value for European clients and citizens, working to empower people, enrich home life, and inspire innovation in organizations of all shapes and sizes. And Huawei is more than committed to making a decisive contribution to Europe's economic recovery. Already today, Huawei has manufacturing sites on European soil. Further significant investments in 5G manufacturing will follow.

To ensure Huawei is able to contribute fairly and equally to the European ICT ecosystem, the company has established thousands of win-win partnerships with European telecoms carriers, industrial companies and industry associations, top universities and research institutes, and local and regional authorities beginning to introduce smart technologies.

Huawei is now a part of the European fabric, an active player in shaping the digital economy for the future, contributing innovative technology to EU research projects and broad-ranging industry-led cooperation initiatives such as those for connected vehicles, digital transformation and smart agriculture.

The EU's approach to free, fair and open competition in the ICT sector, protecting innovation and consumer choice, and ensuring equal opportunities for companies to compete in the European marketplace, makes Europe an attractive base for companies developing high-end intellectual property.