Response to the Public Consultation on the European Commission's White Paper on Artificial Intelligence - A European Approach

Submitted by Prof. Derek McAuley, Dr. Ansgar Koene and Dr. Jiahong Chen of Horizon Digital Economy Research Institute, University of Nottingham

14 June 2020

1. Horizon[1] is a Research Institute centred at The University of Nottingham and a Research Hub within the UKRI Digital Economy programme[2]. Horizon brings together researchers from a broad range of disciplines to investigate the opportunities and challenges arising from the increased use of digital technology in our everyday lives. Prof. McAuley is Director of Horizon and Principal Investigator of the EPSRC-funded DADA[3] (Defence Against Dark Artefacts) project, addressing smart home IoT network security, and its acceptability and usability issues, the ESRC-funded CaSMa[4] (Citizen-centric approaches to Social Media analysis) project to promote ways for individuals to control their data and online privacy, and the EPSRC-funded UnBias[5] (Emancipating Users Against Algorithmic Biases for a Trusted Digital Economy) project for raising user awareness and agency when using algorithmic services. Dr Koene was a lead researcher of the CaSMa and UnBias projects, is Research co-Investigator on the EPSRC-funded ReEnTrust[6] (Rebuilding and Enhancing Trust in Algorithms) project and chairs the working group for developing the IEEE P7003 Standard for Algorithm Bias Considerations. Dr Jiahong Chen is a Researcher Fellow of Horizon, working on the DADA project.

Introduction

2. We welcome the Commission's publication of the AI White Paper, which sets out an EU-wide regulatory strategy to promote innovation and trust in AI for individual benefits and social good. In addition to our responses to the specific questions in the survey, we would like to highlight a number of aspects covered by the survey questions where the further specification and implementation of the White Paper could improve. We would be happy to be contacted for further discussions, and for our comments to be published.

General comments

3. The White Paper has not outlined the scope of "AI" from the outset, which, despite the potential benefit of a flexible, inclusive policy approach in promoting innovation in AI technologies, may leave grave legal uncertainties when regulatory measures are to be introduced. Also, the White Paper has a strong tendency to focus on regulating the "risks" of AI systems. It is of course vital to address the

[1] http://www.horizon.ac.uk
[2] https://epsrc.ukri.org/research/ourportfolio/themes/digitaleconomy/
[3] https://www.horizon.ac.uk/project/defence-against-dark-artefacts/
[4] http://casma.wp.horizon.ac.uk
[5] http://unbias.wp.horizon.ac.uk
[6] https://ReEnTrust.org

substantial threats of AI, but equally important is to monitor the longer-term, less tangible implications for individuals and the society. For example, constantly measuring how different segments of the population may be impacted by certain AI systems – including those deemed to be "low-risk" – should be part of the EU's strategy.

Strengthen excellence in research

4. The Commission's ongoing commitment in supporting investment in AI research and innovation is welcome, but there has been an increasing public concern about the ethics standards of certain EU- or nationally-funded research projects on AI.[7] Maintaining a robust ethics review process for publicly funded AI project is therefore significantly important to ensure responsible research and innovation as well as to promote public trust.

Small and Medium Enterprises (SMEs)

5. One particular form of support that SMEs are likely to demand from Digital Innovations Hubs is sector-specific training on selecting the right AI product/system from a range of available suppliers, as well as creating their own policies to address potential limitations and even risks in the course of deploying "plug and play" AI solutions. This is particularly crucial for SMEs because most of them do not have the necessary resources or skills to differentiate various services with regard to the technical details, not to mention to negotiate with the suppliers for a tailored solution. The fact that many of the AI services are provided on an "as-is" basis also means that SMEs are in a disadvantaged and unmotivated position to anticipate the unintended effects of a particular solution.

Remote biometric identification systems

6. Facial recognition in public spaces has raised serious concerns across Europe for their potential negative effects on individual freedom. While in certain scenarios (such as border control) this can increase efficiency with the impact kept to a minimum level, such uses must be strictly controlled and only permitted on the basis of sector-specific legislation that lays down the necessary safeguards and remedies available to the affected individuals.

Voluntary labelling system

7. A labelling system for AI systems indeed has the potential to support users to make informed decisions choosing the safe and trustworthy products. However, labelling approaches in other regulatory fields (such as food nutrition or energy efficiency labels) have shown that this would sometimes create a false sense of trust and the weakened ability to choose the best-suited product. In this regard, it is of paramount importance that the proposed labelling scheme function not just as an "official seal" for qualified products, but also a useful tool for users to obtain accessible, standardised, and comparable information, and to increase their awareness of the limitations of AI systems. The TRUSTe programme scandal in the US[8] also shows the need for a vigorous accreditation system. The Commission should also consider how the labelling system may be aligned with existing

[7] For example, see https://privacyinternational.org/long-read/3341/monitoryou-millions-being-spent-eu-developing-surveillance-tech-target-you; https://privacyinternational.org/uk-government-funded-ai-programme-wants-make-face-recognition-ubiquitous.

[8] https://www.theguardian.com/technology/2014/nov/18/truste-fine-web-security-seals

certification initiatives in the EU (such as the data protection certification regime under the GDPR) so as to reduce compliance burdens on SMEs.

Liability legal framework

8. As highlighted in the White Paper, AI systems often involve a complex set of actors whose responsibilities are not always clearly defined or fairly allocated. This is particularly the case in the area of product liability, where the exact cause of incidents involving AI systems can be extremely difficult to trace due to the "black-box" nature of some components and the complex structure of the supply chain. This also renders the distinction between producers and suppliers under the Product Liability Directive no longer effective in the market of AI products. A renewed, specialised approach should be therefore introduced to specifically address AI, or indeed any sophisticated electronic systems.

Annex: Responses to the main body of the consultation

Section 1 - An ecosystem of excellence

To build an ecosystem of excellence that can support the development and uptake of AI across the EU economy, the White Paper proposes a series of actions.

In your opinion, how important are the six actions proposed in section 4 of the White Paper on AI (1-5: 1 is not important at all, 5 is very important)?

	1 - Not important at all	2 - Not important	3 - Neutral	4 - Important	5 - Very important	No opinion
Working with Member states	○	○	○	◉	○	○
Focussing the efforts of the research and innovation community	○	○	○	○	◉	○
Skills	○	○	○	○	◉	○
Focus on SMEs	○	○	○	◉	○	○
Partnership with the private sector	○	○	○	◉	○	○
Promoting the adoption of AI by the public sector	○	○	○	◉	○	○

Are there other actions that should be considered?

500 character(s) maximum

Revising the Coordinated Plan on AI (Action 1)

The Commission, taking into account the results of the public consultation on the White Paper, will propose to Member States a revision of the Coordinated Plan to be adopted by end 2020.

In your opinion, how important is it in each of these areas to align policies and strengthen coordination as described in section 4.A of the White Paper (1-5: 1 is not important at all, 5 is very important)?

	1 - Not important at all	2 - Not important	3 - Neutral	4 - Important	5 - Very important	No opinion
Strengthen excellence in research	○	○	○	○	◉	○
Establish world-reference testing facilities for AI	○	○	○	○	◉	○

Promote the uptake of AI by business and the public sector	○	○	○	◉	○	○
Increase the financing for start-ups innovating in AI	○	○	○	◉	○	○
Develop skills for AI and adapt existing training programmes	○	○	○	○	◉	○
Build up the European data space	○	○	○	◉	○	○

Are there other areas that that should be considered?

500 character(s) maximum

Strengthening ethics reviews for EU-funded AI research projects. (See para 4 attachment)

A united and strengthened research and innovation community striving for excellence

Joining forces at all levels, from basic research to deployment, will be key to overcome fragmentation and create synergies between the existing networks of excellence.

In your opinion how important are the three actions proposed in sections 4.B, 4.C and 4.E of the White Paper on AI (1-5: 1 is not important at all, 5 is very important)?

	1 - Not important at all	2 - Not important	3 - Neutral	4 - Important	5 - Very important	No opinion
Support the establishment of a lighthouse research centre that is world class and able to attract the best minds	○	○	○	○	◉	○
Network of existing AI research excellence centres	○	○	○	○	◉	○
Set up a public-private partnership for industrial research	○	○	○	◉	○	○

Are there any other actions to strengthen the research and innovation community that should be given a priority?

500 character(s) maximum

Focusing on Small and Medium Enterprises (SMEs)

The Commission will work with Member States to ensure that at least one digital innovation hub per Member State has a high degree of specialisation on AI.

In your opinion, how important are each of these tasks of the specialised Digital Innovation Hubs mentioned in section 4.D of the White Paper in relation to SMEs (1-5: 1 is not important at all, 5 is very important)?

	1 - Not important at all	2 - Not important	3 - Neutral	4 - Important	5 - Very important	No opinion
Help to raise SME's awareness about potential benefits of AI	○	○	○	◉	○	○
Provide access to testing and reference facilities	○	○	○	◉	○	○
Promote knowledge transfer and support the development of AI expertise for SMEs	○	○	○	○	◉	○
Support partnerships between SMEs, larger enterprises and academia around AI projects	○	○	○	◉	○	○
Provide information about equity financing for AI startups	○	○	○	◉	○	○

Are there any other tasks that you consider important for specialised Digital Innovations Hubs?

500 character(s) maximum

To provide training on managing AI-related risks in selection and deployment of AI systems. (See para 5 attachment)

Section 2 - An ecosystem of trust

Chapter 5 of the White Paper sets out options for a regulatory framework for AI.

In your opinion, how important are the following concerns about AI (1-5: 1 is not important at all, 5 is very important)?

	1 - Not important at all	2 - Not important	3 - Neutral	4 - Important	5 - Very important	No opinion
AI may endanger safety	○	○	○	○	◉	○
AI may breach fundamental rights (such as human dignity, privacy, data protection, freedom of expression, workers' rights etc.)	○	○	○	○	◉	○
The use of AI may lead to discriminatory outcomes	○	○	○	○	◉	○
AI may take actions for which the rationale cannot be explained	○	○	○	○	◉	○
AI may make it more difficult for persons having suffered harm to obtain compensation	○	○	○	○	◉	○
AI is not always accurate	○	○	○	○	◉	○

Do you have any other concerns about AI that are not mentioned above? Please specify:

500 character(s) maximum

AI may reinforce existing social injustice or economic inequality.

Do you think that the concerns expressed above can be addressed by applicable EU legislation? If not, do you think that there should be specific new rules for AI systems?

- ○ Current legislation is fully sufficient
- ○ Current legislation may have some gaps
- ◉ There is a need for a new legislation
- ○ Other
- ○ No opinion

If you think that new rules are necessary for AI system, do you agree that the introduction of new compulsory requirements should be limited to high-risk applications (where the possible harm caused by the AI system is particularly high)?

- ◉ Yes
- ○ No
- ○ Other
- ○ No opinion

Do you agree with the approach to determine "high-risk" AI applications proposed in Section 5.B of the White Paper?

- ○ Yes
- ◉ No

○ Other
○ No opinion

If you wish, please indicate the AI application or use that is most concerning ("high-risk") from your perspective:

500 character(s) maximum

In your opinion, how important are the following mandatory requirements of a possible future regulatory framework for AI (as section 5.D of the White Paper) (1-5: 1 is not important at all, 5 is very important)?

	1 - Not important at all	2 - Not important	3 - Neutral	4 - Important	5 - Very important	No opinion
The quality of training data sets	○	○	○	◉	○	○
The keeping of records and data	○	○	○	◉	○	○
Information on the purpose and the nature of AI systems	○	○	○	○	◉	○
Robustness and accuracy of AI systems	○	○	○	○	◉	○
Human oversight	○	○	○	○	◉	○
Clear liability and safety rules	○	○	○	○	◉	○

In addition to the existing EU legislation, in particular the data protection framework, including the General Data Protection Regulation and the Law Enforcement Directive, or, where relevant, the new possibly mandatory requirements foreseen above (see question above), do you think that the use of remote biometric identification systems (e.g. face recognition) and other technologies which may be used in public spaces need to be subject to further EU-level guidelines or regulation:

○ No further guidelines or regulations are needed
○ Biometric identification systems should be allowed in publicly accessible spaces only in certain cases or if certain conditions are fulfilled (please specify)
○ Other special requirements in addition to those mentioned in the question above should be imposed (please specify)
◉ Use of Biometric identification systems in publicly accessible spaces, by way of exception to the current general prohibition, should not take place until a specific guideline or legislation at EU level is in place.
○ Biometric identification systems should never be allowed in publicly accessible spaces
○ No opinion

Please specify your answer:

Such technologies should be limited to specific contexts and allowed only when special safeguards have been provided in sector-specific legislation. (See para 6 attachment)

Do you believe that a voluntary labelling system (Section 5.G of the White Paper) would be useful for AI systems that are not considered high-risk in addition to existing legislation?

- ○ Very much
- ◉ Much
- ○ Rather not
- ○ Not at all
- ○ No opinion

Do you have any further suggestion on a voluntary labelling system?

500 character(s) maximum

An effective labelling system would not just involve recognition of "safe" products but also support consumers to make comparisons and identify potential risks. (See para 7 attachment)

What is the best way to ensure that AI is trustworthy, secure and in respect of European values and rules?

- ☐ Compliance of high-risk applications with the identified requirements should be self-assessed ex-ante (prior to putting the system on the market)
- ☑ Compliance of high-risk applications should be assessed ex-ante by means of an external conformity assessment procedure
- ☑ Ex-post market surveillance after the AI-enabled high-risk product or service has been put on the market and, where needed, enforcement by relevant competent authorities
- ☑ A combination of ex-ante compliance and ex-post enforcement mechanisms
- ☐ Other enforcement system
- ☐ No opinion

Do you have any further suggestion on the assessment of compliance?

500 character(s) maximum

Section 3 – Safety and liability implications of AI, IoT and robotics

The overall objective of the safety and liability legal frameworks is to ensure that all products and services, including those integrating emerging digital technologies, operate safely, reliably and consistently and that damage having occurred is remedied efficiently.

The current product safety legislation already supports an extended concept of safety protecting against all kind of risks arising from the product according to its use. However, which particular risks stemming from the use of artificial intelligence do you think should be further spelled out to provide more legal certainty?

- ☑ Cyber risks
- ☑ Personal security risks
- ☑ Risks related to the loss of connectivity
- ☑ Mental health risks

In your opinion, are there any further risks to be expanded on to provide more legal certainty?

500 character(s) maximum

Do you think that the safety legislative framework should consider new risk assessment procedures for products subject to important changes during their lifetime?

- ◉ Yes
- ○ No
- ○ No opinion

Do you have any further considerations regarding risk assessment procedures?

500 character(s) maximum

Do you think that the current EU legislative framework for liability (Product Liability Directive) should be amended to better cover the risks engendered by certain AI applications?

- ◉ Yes
- ○ No
- ○ No opinion

Do you have any further considerations regarding the question above?

500 character(s) maximum

The concepts such as "producer" and "supplier" need to be renewed to reflect the nature of AI systems and the structure of the ecosystem. (See para 8 attachment)

Do you think that the current national liability rules should be adapted for the operation of AI to better ensure proper compensation for damage and a fair allocation of liability?

- ○ Yes, for all AI applications
- ◉ Yes, for specific AI applications
- ○ No
- ○ No opinion

Please specify the AI applications:

Strict liability or no-fault compensation schemes should be considered for such products as self-driving vehicles and robots (or "cobots") in the workplace.

Do you have any further considerations regarding the question above?

500 character(s) maximum