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

[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

a strong tendency to focus on regulating the "risks" of AI systems. It is of course vital to address the 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

[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.

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 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.

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