Broadcom's feedback on the European Commission AI Inception Impact Assessment

Introduction

Broadcom would like to thank the European Commission for launching this public consultation. We believe that the inception impact assessment is asking the right questions and presents a reasonable list of alternatives to consider.

We believe we have a unique perspective to bring in the AI discussions because of the diversity of businesses Broadcom is currently engaged in. Broadcom is known for semiconductors manufacturing that is AI-enabled. In addition, Broadcom is using and building AI capabilities in several of its software businesses, for purposes such as information technology (IT) infrastructure management, in support of mainframe technology mostly for financial services, in cybersecurity to detect, prevent and mitigate cyberattacks as well as in payment security to detect and prevent financial fraud. Our unique perspective comes from the different use cases and benefits AI brings as well as the feedback of our customers in using and deploying our AI technology.

Broadcom agrees with the Commission that AI can bring considerable benefits to Europe. Broadcom believes that it is possible to manage the risks associated with the introduction of any new technology like AI in a pragmatic, cost-effective and market friendly manner that could make Europe a strong regulator and a competitive market for the development of AI. Broadcom encourages the Commission to take into account in the development of an EU framework how other regulators in the US and UK are tackling AI challenges in order to ensure regulatory compatibility and a market for European AI products that will scale beyond the EU.

Our comments in more detail

Whereas we agree with many of the comments and observations made in the inception impact assessment we would like to highlight certain areas we believe are important as well as to challenge certain assumptions that we think could benefit from additional considerations. We believe that considering the potential for innovation, speed of dissemination, wide reach, network effects and potential impact of the technology industry in the European society, any EU initiatives on AI should equally apply to large enterprises and SMEs that would both benefit from a clear regulatory framework and the strong brand recognition it would deliver.

Cost of the different options

The impact assessment takes the view that the option with less costs is voluntary labelling. Instinctively that sounds true but in practice it may turn out not to be. The voluntary nature of the labelling means that organizations choose whether to subject themselves to the labelling process. That in itself reduces the cost because it is a choice to label or not to label. However, if the labelling system proves effective because it is widely market-adopted or because the EU has assigned specific incentives to using a label then the labelling system becomes a de-facto criterion to enter the market. That in of itself is not negative provided that the labelling system is set up in such a way to address concerns like speed to enter the market (and get the label) or the need to update/patch or modify the AI product (in the case of software). We analyse this point in detail in our feedback on the white paper. All this assumes the existence of a single voluntary labelling scheme. If multiple labelling schemes were to emerge, whereas the competition may be welcomed there is a risk of fragmentation and confusion that defeats the purpose of the label.

The impact assessment takes the view that Option 3, the fully-fledged regulatory approach, is the most expensive one. Again, instinctively this is correct, but there are ways to minimize the cost, assuming that this would be the preferred option. More specifically the impact assessment talks about requirements in Option 3 such as documentation and record keeping, training, accuracy, etc. Whereas some of these requirements are very reasonable for high risk applications, we would caution the Commission to avoid repeating some of the provisions of GDPR that were well intended but, in the end, produce more paper compliance than actual

privacy-friendly effects. Several of the record keeping requirements of GDPR produce a paper-trail that may be useful to demonstrate compliance, but it will be relevant only in the case of an investigation, does not really add up to meaningful privacy protection, while it triggers considerable costs linked with internal processes and cycles. None is against keeping records of risk assessments or documenting how/why decisions are made but there should be a purpose and use of such records beyond "just in case". This is especially important when concerning live products or production data such as training data and algorithms in the case of AI.

Scope of application

We agree with the Commission that if the decision is to go down the regulatory option, then the focus of regulatory action should be on sub-option (b) of option 3, i.e. the high-risk applications. We believe that legislation in this area should follow a risk-based approach and such an approach must take into account the context when assessing the risk, the impact of such risk occurring but also the probability of such occurrence. Therefore, specific use cases need to be called out and not just a broad class of application or technology. For these reasons any additional regulation should focus on a narrow definition of AI systems which would focus on high-risk AI applications. The determination of high-risk should combine sector, impact but also to the degree possible, the probability of harm based on experiences of incidents that have occurred as a result of introduction of new technologies. Clearly some sectors standout such as transport, health and energy. Harm should not be considered only through the perspective of an individual but needs to take a balanced approach of broader societal goods, benefits and risks. There may be great societal benefits to be gained in a case of a pandemic by using AI to process certain categories of data to advance public health. Equally, other types of harm to be considered and avoided through the use of AI could be environmental harm, economic/financial harm, critical infrastructure disruption and service degradation.

The requirements linked with high risk applications should vary depending on the nature of the AI system. Given the plethora of applications it is very difficult for one-size to fit all. At the very least however they should include outcome driven requirements around data quality, security, robustness and a reasonable level of transparency/explainability without that necessarily resulting in full disclosure. Emphasis should also be put on testing output to ensure verifiability of the results and a reasonable level of quality especially if the AI is expected to further "self-develop" with data from the field.

Proximity and usage of real-life data should be encouraged as a mechanism of quality. It is critical to ensure that AI in Europe is trained on data available from different parts of the world as opposed to training or retraining on just European data. An AI that is trained with global real-life data sets is more likely to be effective, accurate and suitable for a number of applications that are global by nature e.g. cybersecurity or fraud prevention. It is also less likely to be discriminating or to result in less accurate outcomes. It would also be easier to export thus helping Europe to achieve its ambitions on tech leadership.

A lot of discussion has taken place over the need to protect fundamental human rights from AI decision making that may be biased or result in different forms of profiling and surveillance. The concerns are justifiable and are well understood. AI is already used nowadays for certain forms of pattern recognition in order to manage large amounts of data and identify patterns of specifically targeted risk indicators. The critical element here is the language used in GDPR Articles 4.4 and 22 around profiling and automated decision making.

A lot of AI is used to create profiles of behaviour that are not linked to a particular individual yet the parameters of such behaviour are used to indicate that certain actions are needed or that certain risks occur. Cybersecurity and fraud prevention are typical examples. The security teams do not need to be aware of who is performing certain actions but rather that the actions performed fall within the envelop of what would be characterised as potentially fraudulent behaviour. Such processing although automated and potentially involving the creation of a profile of certain behavioural characteristics is not in itself "usage of personal data to evaluate certain personal aspects relating to a natural person" because they do not relate to a specific identifiable individual nor do they "analyse or predict aspects concerning a natural person's performance at work, situation, health, personal preferences, interests, reliability, behaviour, location or movements". In addition, such processing is not going to have legal or similarly significant effects (usually). The more likely

scenario in such situations is that a credit card transaction will be denied or a connection to a network will be blocked.

Liability and conformity assessment

AI systems become customized and evolve as a result of continuous training serving particular customers and markets. The training would be based on the specific business needs, location and business model. Consequently, any legal obligations and associated liabilities concerning an operational AI system should apply to the operator-user of the system that has further trained and evolved the AI as opposed to the original producer or the service provider that acts under the instructions of the operator-user. The use of AI systems and therefore any resulting liability is going to be context-specific and may involve a complex supply chain. This is why having more than a single operator/user who is liable or introducing joint liability is not going to be workable. Suppliers of the underlying high-risk technology should be able to provide attestations of its fitness for purpose, while end-users of a specific AI application should ensure (especially if they further develop the AI using custom data sets) fair use of the technology.

Imposing ex-ante conformity assessment for AI systems creates a disproportionate barrier to enter the market. This barrier would be particularly significant for SMEs that may want to innovate using AI. The barrier would also function as an obstacle to bring technologies into the market and can negate a first mover advantage that European companies may have when taking advantage of a clear framework in Europe. We would support a system that combines ex-ante self-assessment for high-risk applications, followed by ex-post market surveillance. For more detail on the issues arising on this please see our detailed comments on the White Paper.

++++++++++++++++++++

We would like to thank the European Commission for giving us the possibility to provide feedback to this important issue that we believe will have a major impact in the development of technology policy in the European Union.

We remain at your disposal to provide additional information. Please feel free to contact:

Ilias Chantzos, LLM, MBA

Global Privacy Officer and Head of EMEA Government Affairs

Ilias.chantzos@broadcom.com