European Commission White Paper on Artificial Intelligence
A European approach to excellence and trust

Draft comments from Motorola Solutions

Motorola Solutions is a global leader in mission critical communications and analytics. Our technology platforms in mission critical communications, command center software and video security, bolstered by managed and support services, make cities safer and help communities and businesses thrive. We serve over 100,000 public safety and commercial customers in more than 100 countries, with an install base of over 13,000 systems and a global footprint of 17,000 employees worldwide, and have a rich heritage of innovation spanning over 90 years. In 2019, we invested US $687 million in research and development, and as of December 31, 2019, we had approximately 6,000 employees engaged in R&D activities.

Motorola Solutions welcomes the opportunity to submit comments on the proposals in the European Commission's White Paper on Artificial Intelligence, *A European approach to excellence and trust*.

Motorola Solutions strongly support many of the positions and ambitions set out in the White Paper:

- The need for stable, consistent regulation/laws across the EU, that avoid stifling innovation, and establish an EU-wide regulatory environment. This would provide scale and efficiency for high quality, responsible and thorough AI product development, and facilitate transparency and trust in AI. As described below, we believe that this would be best accomplished by individual sectors considering implications of AI for their domain, rather than by a generic regulatory framework.

- The value of an ecosystem of trust as a foundation for AI, including human-centered design. Our users rely upon our technologies to deliver public safety, and for their business and/or personal safety. Many are public servants, so societal trust is essential for their work and tools they use. Human oversight is central to our philosophy, and a good mitigation for high risk AI applications. We are now using design and human factors as fundamental guidelines that we develop with our users' use-cases and circumstances in mind. There may be generic human centered design guidelines that could be developed centrally - perhaps as a research endeavor to address current limitations, such as ensuring the human stays in the loop cognitively and effectively(to avoid 'AI blindness') - and tailored to existing structures or focus area (pharma, finance, public safety, etc).

- Developing a risk framework and risk-based approaches. The parameters of severity/likelihood are the right vectors to characterize risk. It would help to promote consistent values/thinking, transparency, and careful AI application if a risk-based framework could be created, for use by actors in specific sectors to leverage in their application of AI within their sector.

- Actions to encourage adoption of AI by the public sector. We recommend including Public Protection and Disaster Relief, and Security, in the list of priority sectors for dialogue denoted in Action 6 in Section 4 F, since safety is one of the clearly stated, societally visible, benefits of AI.

- Investing in research, and making edge/low-power computing and AI a focus for the EU. Our solutions are generally deployed in a mobile setting, or are deployed devices (cameras, vehicles). A key application of AI for Motorola Solutions is on the edge - for example, camera-resident video analytics, natural language processing, and sensors in a PAN/VAN ecosystem.

- Encouraging, creating and curating common, meaningful data sets for training purposes, that can be applied and leveraged across many products and applications, and that ensure demographic representation, consistency, quality, privacy, etc, to avoid issues such as bias. Biometric datasets can be used for authentication/identification in many applications, as well as for security. Natural language datasets such as voice interaction have wide applicability (and demographic variability across different languages, dialects, etc). Benchmarks for common cases (e.g. facial recognition accuracy, speaker word/intent recognition) could be developed objectively. Providers could be tested or self-certify. This could provide a basis for the 'voluntary labeling system' in Section 5.

- Encouraging and structuring product controls, measures, recording and accountability methods - to be tailored and applied in the context of specific use cases and domains, we suggest. We further consider that it would be useful to develop best practices, techniques and frameworks, for individual industries and applications to tailor for their specific sectors and use cases.

Our main observations on the White Paper concern a future EU regulatory framework. We do not believe that AI can be effectively regulated as a broad technology. It would be difficult, if not impossible, for a single framework to deal with all the diverse challenges of the wide range of application areas for AI. An approach based on generic regulation would risk stifling development; would entail difficulties over definitions in a fast-changing landscape; and would be neither agile nor meaningful, if treated separately from the context of the specific use. In our view, the risk factors around AI are not universal, and depend on a range of possible mitigations - for example technical, application or process-based.

We recommend that AI should be evaluated in the context of the domains where it is used, alongside existing laws and regulations. One practical and effective approach might be to have multiple levels of controls, for example different levels of requirements based not just on potential risk, but also the size of the industry. This could give more flexibility at early stages of development, and become more restrictive as the industry grows, if warranted. It could automatically trigger creation of specific rules for the area, on the basis that it is impossible to predict all future possibilities from the start of development.

We believe that significant, generic legislation on AI should be avoided. To the extent that any AI-specific legislation is introduced, it should be limited, so as not to hinder technology development. We consider the White Paper's stated aim - that the definition of AI should be sufficiently flexible to accommodate technical progress, while being precise enough to provide the necessary legal certainty - would be very difficult to achieve. It is very difficult for any abstract legislation governing technology to contemplate all applications, outcomes, use cases and future derivatives and accommodations. The definition of AI that is referenced in footnote 47 on page 16 of the White Paper highlights this difficulty: algorithmic outcomes and computer vision would fit within this definition, but would not necessarily be AI.

To avoid being overly restrictive/oppressive for some AI uses, and superfluous for others, we recommend that any new legislation should instead be enacted or extended in the context of existing frameworks that apply to specific sectors or fields of use (finance, pharma, etc). We recommend that the EU consider developing a legal and/or regulatory framework that could then be considered in the context of each domain, and tailored as necessary to extend regulation/legislation that already applies to that domain.

In relation to the existing EU legislative framework relating to AI, and the changing functionality of AI systems, it is true that field deployed machine learning can change behavior. However, it has been true for decades that software upgrades can change a system's functionality, irrespective of AI. We advise against extending the scope of AI regulation into these realms. Other factors are at play, and industry has dealt with these challenges for a long time, through testing, incremental deployment (Beta versions), and other software quality control methods. These approaches are well-established and effective.

With regard to Compliance and Enforcement, the White Paper proposes a prior conformity assessment process, to verify and ensure compliance with any mandatory requirements for high-risk applications. We believe several application or domain-specific factors weigh against this approach. They include:

- ○ The need to balance the positive impact of AI for specific outcomes (eg safety and security).
- ○ Constraints around the use of AI applications (eg human validation), and/or compliance and audit controls to enforce and/or create accountability for the proper use of AI.
- ○ Specific impacts of a given application. For example, not all forms of biometric identification using facial recognition are necessarily 'high risk' - eg benign applications for access control.

We believe periodic checks may not be reliable for fielded machine learning, since systems can face new or different circumstances. We also consider it unlikely that independent conformity testing/assessment would work well at scale and across all possible applications of AI. Because outcomes of AI are related to existing outcomes through 'conventional' means, it would make more sense to have each sector (pharma, finance, safety/security, etc.) interpret and apply the risk framework in its own context, and develop appropriate limits, restrictions, certification, testing, mitigation, etc. Existing frameworks are best-suited to establish the most appropriate legal structure for application of AI within their sectors.

Any new 'governance structures' should focus on broad topics that can be applied in each domain - eg customization risk framework, common data sets, benchmarks/test, design considerations, core research to provide tools to improve transparency, etc. They could also focus on development of best practices and standards for compliance controls, audits, transparency, etc.

Finally, we recommend the follow areas for consideration in further EC work on this subject:

- Fostering EU-wide emphasis on common aspects of AI that apply broadly, including:
  - ○ Best practices/standards for compliance controls, audits, transparency, process frameworks.
  - ○ The Risk Framework, including risk mitigation, and issues that need special attention or to be avoided (e.g., fielded machine learning).
  - ○ Curated, representative and robust common training data sets.
  - ○ Research for common tools/methodologies (e.g., to facilitate transparency, testing, etc).
  - ○ EU-wide advocacy for consistent regulation/legislation across countries.

- Engaging directly with the Public Protection and Disaster Relief (PPDR) community, including both industry and user groups, to consider their unique needs, circumstances and existing legal frameworks, and to help to unify related aspects across countries.

- Developing a public education campaign to demystify and ease concern over the application of AI, that individual sectors could build on as AI is applied to their domain. This could include common indicators, notifications, and self-certification methods that could be broadly applied. for cases that span many applications such as Natural-Language Understanding, facial/biometric recognition, etc.