**Alliance for
Internet of Things
Innovation**

Brussels, 24/02/2022

AIOTI Views on Artificial Intelligence Liability

With AIOTI being a multi-stakeholder community where its members have different roles, positions and perspectives in the various IoT and related digital ecosystems, sectorial and otherwise, it has a holistic, system approach. Furthermore, IoT devices, systems and other projects generally include multiple connectors and other components from multiple vendors, including for instance data providers, software providers, identity providers and service providers (to name a few), either upstream, midstream, or downstream in the value ecosystems. This for once means that not all legal or contractual relationships within scope of the Product Liability Directive (PLD) are or will not always be bilateral. A more holistic, system-approach therefore regarding PLD and related matters is therefore recommendable, especially regarding AI – parts of which algorithms, datasets and components may be from multiple of such providers, both during the data life cycle as well as product or related cyber-physical system life cycle. Liability in AI context, as well as the burden of proof, therefore, is not binary.

As AIOTI we strongly believe in a human-centered AI: AI must not replace human intelligence but rather augment our intelligence. As such, AI should not take final decisions in high-risk situations, and there should be the transparency, accountability and human oversight in all situations where AI presents ethical concerns, offering options to clearly (ex-ante) explain and inform a decision to be made by a human. In terms of liability, if these options are provided in an auditable and accountable way this human-centered approach should not place full responsibility on an AI system when a human ultimately took the well-informed decisions.

Horizontal approaches to liability may not be suited to AI, where non-horizontal context matters. We believe that a one-size-fits all approach to AI liability would not fit the AI value chain, which encompasses a broad set of technologies, applications and uses with unique specificities and implications.

Harmonizing the liability regimes on EU level would have negligible impacts on distribution models. Harmonisation and a high protection level is already achieved by Machinery Regulation, the Artificial Intelligence Act and the proposed General Product Safety Regulation, however we recommend and would support additional Guidance of the European Commission on the interplay of these regulations

A potential harmonised insurance obligation should be laid down at EU level, only in fields where no mandatory liability insurance exists yet, for using AI products and providing AI-based services that pose a serious injury risk (e.g. life, health) to the public.

Example: Mandatory liability insurance for cars on the road already exists and covers damages resulting from embedded AI; when the car has embedded AI for autonomous driving, that would not change the height of the damage a car accident could cause – when at the same time embedded AI makes the chance on an accident smaller – eg no drunken drivers…

C2 General

Manufacturer will take various 'buildings blocks' into account to generate trustworthiness of AI systems. Those building blocks are related to technical and non-technical requirements related to data evaluation, data quality, supply chain, training procedures, pre-defined boundary conditions, software development life cycle SDLC, implementation, performance, robustness, resilience, privacy, user training, and many others. Manufacturer shall be able to demonstrate accountability by demonstrating compliance to requirements laid out in related European or international standards and certification schemes.

From our perspective, it would be preferable to focus first on rules around conformity assessment within the existing framework and promote the adherence to technical standards throughout the value chain as the basis for an efficient and transparent distribution of liability. The further maturing of AI technology on the EU market together with the development of certification schemes will be the most efficient path to improve consumer protection, increase trust in emerging technologies and support the development of innovative companies. It is essential for legal certainty as well as harmonisation of regimes that technical standards and certification schemes are recognised as a key element for the distribution of liability rather than potentially broad concepts.

The consultation mainly refers to "possible problems" and elements that "may create challenges" for consumers to obtain compensation for damages. Therefore, it is unclear whether obstacles justify a substantial revision of the PLD. A revision of the PLD requires strong evidence that the current framework does not adequately allow consumers to seek compensation for damages caused by a digital product.

We are concerned that an expansion to standalone software would fail to consider the specific characteristics of software and potentially hamper the uptake of innovative AI-driven solutions. The PLD is technology-neutral that applies to all products, including defective products that are software-enabled. The current framework can therefore apply to new products without a need for significant changes in the legislation.

Applying strict liability to stand-alone software and AI systems is disproportionate as they are significantly different from other products under the Directive: they can be multi-purpose, their functioning depends on their specific use and user, and they are often services-based. Applying strict liability for general purpose software would be especially ill-suited, since their exact use, application, purpose is decided by users and cannot be known in advance.

We call on the European Commission to ensure that the incoming legislation on AI liability aligns with the ongoing legislative processes on draft proposals like the AI Act and the Digital Services Act which include product safety rules and key elements including how to define AI systems, types of risks and the allocation of responsibilities in the AI value chain and further obligations on algorithmic design and transparency. Thus, multiplying legislative frameworks might lead to a burdening complexity for SMEs when it comes to assessing risks and compliance needs of their products. Most of them do not have sufficient legal resources and expertise to navigate and apply overlapping requirements. Moreover, we fear that a lack of clear definition of AI systems will have negative an impact on determining liability and might not be suited to the complex nature of AI solutions, which involves a highly iterative process, experimentation and a multi-stakeholder approach (3rd party developers, deployers and users).

C2 General

We recommend to carefully consider the policy options and contextuality to shifting the burden of proof, consider the contextuality (as in certain scenarios is may make sense where in others it could be established as disproportionate evidence fishing or similar), and identify and examine possible alternatives – some of which are already deployed such as for instance the right to seize evidence with assistance of a trusted third party (being a process service and expert IT auditor) as is possible in the Netherlands –. Where defect and causation may be the relative less difficult phase, proving the existence of damage in AI-related occurrences will continue to be a challenge for consumers, whether the burden of proof may or may not be shifted in particular cases.

About AIOTI

AIOTI is the multi-stakeholder platform for stimulating IoT Innovation in Europe, bringing together small and large companies, start-ups and scale-ups, academia, policy makers and end-users and representatives of society in an end-to-end approach. We work with partners in a global context. We strive to leverage, share and promote best practices in the IoT ecosystems, be a one-stop point of information on all relevant aspects of IoT Innovation to its members while proactively addressing key issues and roadblocks for economic growth, acceptance and adoption of IoT Innovation in society.

AIOTI's contribution goes beyond technology and addresses horizontal elements across application domains, such as matchmaking and stimulating cooperation in IoT ecosystems, creating joint research roadmaps, driving convergence of standards and interoperability and defining policies. We also put them in practice in vertical application domains with societal and economic relevance.

AIOTI is a partner for the European Commission on IoT policies and stimulus programs, helping to identifying and removing obstacles and fast learning, deployment and replication of IoT Innovation in Real Scale Experimentation in Europe from a global perspective.

AIOTI is a member driven organisation with equal rights for all members, striving for a well-balanced representation from all stakeholders in IoT and recognizing the different needs and capabilities. Our members believe that we are the most relevant platform for connecting to the European IoT Innovation ecosystems in general and the best platform to find partners for Real Scale Experimentation.

C2 General