ITI Promoting Innovation Worldwide

# ITI's views on

# Adapting Liability Rules to the Digital Age and Artificial Intelligence

10 January 2022

## Introduction

ITI, the Information Technology Industry Council, welcomes the opportunity to provide input to the European Commission on the revision of Liability Rules. As the premier global advocate for technology, representing 80 of the most innovative companies in the world, ITI recognises the importance of achieving a liability regime that addresses potential challenges that may arise as a result of the digital transformation and from new technologies such as Artificial Intelligence (AI).

However, it is too early at this stage to engage in a revision of the Product Liability Directive (PLD) to specifically account for the challenges posed by new technologies such as Artificial Intelligence, as this work should be based on solid evidence of proven flaws and consumer harm in the current framework – evidence that has not been presented to date. We caution against proposals to include software and services in the scope of the PLD, as this would fail to take into account the specific characteristics of software and potentially damage innovation. It is important to note that software and, in particular, AI are not a product by themselves, but are rather components of a product or a service, and as such should be treated. Finally, given the ongoing legislative work on the AI Act, we recommend waiting until the new framework is finalised, so that the concepts contained therein are fully crystallized and understood.

The following comments address more specifically the different policy options laid out in the public consultation.

## Section I - Revision of the Product Liability Directive (PLD)

The Product Liability Directive (PLD) has empowered European consumers to seek compensation for damages caused by defective products for the past 30 years. The Directive has proven to be a technology-neutral tool striking the right balance between the obligations for consumers and producers, thereby creating legal certainty in the Single Market. For this reason, we caution against revising the legislation without first having found solid evidence that innovative technologies have harmed consumers in a way that the PLD or other legislation has not sufficiently allowed for redress. If such evidence is presented, policymakers should then decide on required legal steps and whether a revision of or addition to the PLD is justified. In addition, legislation in the field of Data Protection already provides meaningful pathways for redress for privacy and personal-data-related matters arising from the use of

*Global Headquarters*
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

*Europe Office*
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

new technologies such as AI. Finally, it is unclear how a potential revision of the PLD to specifically account for potential challenges posed by AI technologies would interact with the proposed AI Act, whose main concepts and terminology are still under discussion with the co-legislators. Also, the AI Act aims to further increase safety of products and services, which could in turn positively impact consumer harm and resulting claims. We thus suggest that any potential revision of the PLD should take place after the adoption of the AI Act, so as to ensure that the two frameworks remain aligned and complementary. Therefore, as regards the question in page 23 of the questionnaire asking the preferred policy option, ITI believes that no legislative change is necessary at the moment.

**Digital content**

The consultation argues that it is unclear how the existing framework of the PLD applies to "digital content, software and data, especially when supplied separately from a tangible product," in the event a "digital" defect leads to damage (p.9-10). **We caution against including standalone software in the scope of the PLD** as this would fail to take into account the specific characteristics of software, which differ from physical products. Software can be deployed in a variety of ways and its characteristics depend strongly on how they are being used. The existing PLD already provides safeguards against defective products, regardless of whether they are equipped with software, but refrains from liability provisions for stand-alone software which a user downloads and uses. Moreover, national jurisdictions on liability already cover products which include software. Expanding legal exposure to software developers and others playing an intermediate role in the value chain would be disproportionate. In any event, there are substantial existing statutory protections for consumers at EU and national levels, including the ability to bring claims in tort and contract law. In addition, the implementation of EU 2019/770 and 771 has provisions related to liability and software updates (applicable to product conformance/consumer contracts). Therefore, a possible revision of the Product Liability Directive could lead to redundant or conflicting requirements and add additional complexity and financial costs for companies and, ultimately, cause legal uncertainty. To the extent that liability rules are deemed insufficiently clear in case of products with embedded software, the question of how to make these rules better understandable to consumers and providers across Member States should be discussed in more detail.

**Software in general, and AI specifically, rely on complex supply chains that include multiple actors throughout its lifecycle.** These include developers, the deployer and potentially others (producer, distributor or importer, professional or private user). It is also common that some of these actors may not be aware of the existence/role of other actors or may be unaware of the ways in which another actor might be using their products or services. As such, it is unclear how the strict liability regime of the PLD would be distributed among the actors involved where it is unclear who should be treated as a "producer". The fact that many of these concepts related specifically to the actors in the AI supply chain are still being debated in the context of the AI Act also raises concerns about potential legal uncertainty.

Of particular concern would be the implications for **the open-source community**, which is key to the rapid advancement of software and AI technologies. Many services and software

systems, including AI systems, are the result of numerous entities building on top of others' efforts. These systems often start with open-source libraries, tools, and frameworks, created by hundreds or thousands of contributors offering bits of code which can be large or small. Those open-source libraries, tools, and frameworks might then be combined with open data sets that themselves might be the work of hundreds or thousands of other people. And the resulting piece of software or AI model might then be shared under an open-source license for others to build on. While there are practical concerns on how the strict liability framework may apply to such ecosystem, it is also important to note that applying strict liability to every open-source contributor would create huge disincentives to open-source software development, severely undermine the open-source ecosystem that has been critical to AI development and especially disincentivise smaller developers from taking part in AI innovation.

There are also elements related to user responsibility that need to be considered. Should strict liability apply where a consumer has not taken reasonable measures to apply software updates, or has not used software according to instructions, and damage occurs as a result, this would extend the scope beyond the current PLD and existing case law. This would ultimately increase the risk for third party developers, disincentivising innovation in development.

If Europe were to become the first global player to apply strict liability to services and software, the roll-out and uptake of AI-based technologies would also be hindered, impacting businesses and start-ups operating in Europe and coming into conflict with the stated goals of the Commission to encourage innovation and create an ecosystem of excellence in Europe. Strict liability is a powerful tool which should only be used for a very limited number of cases. Introducing strict liability for software and AI-based technologies would disproportionately spread liability throughout the supply chain, also exposing to liability actors that could not and should not reasonably be expected to bear responsibility for situations beyond their control.

It is also unclear how strict liability would interact with other specific examples of intangible elements included in the consultation (p.10). The consultation mentions, for instance, **training data and other types of data (such as "data that comprises only information")**. In the case of training data, it is unclear how a dataset would be considered defective. In many cases, it is impossible to identify and eliminate all errors in a data set. In some cases, it may be more useful for models to learn with errors in the data, so they become more robust and better able to handle data encountered in the real world, which is unlikely to be sanitized and perfectly accurate. All software and computer systems, including AI, will always contain bugs. Even the most complete coding process with associated QA controls cannot possibly identify all bugs prior to deployment. Most importantly, "data" alone do not cause harm but possibly the context how they are used, such as within a product. The PLD sufficiently covers harm resulting from defective products, including defects of products that related to problems with data.

**Online marketplaces**

The consultation asks whether online marketplaces should be considered importers under the Product Liability Directive when there is no EU-based importer or producer (p. 12-13). ITI

agrees that the objective of consumer protection is paramount, and consumers should be offered effective pathways for obtaining compensation. As also mentioned in the questionnaire, it is fundamental here to consider how any extension of the scope of the PLD would interact with ongoing conversations on seller identification in the context of the Digital Services Act (DSA) and General Product Safety Regulation (GPSR), and ensure that approaches to intermediaries liability are coherent.

Regulation 2019/1020 "on market surveillance and compliance of products" also created a new obligation for products placed on the EU market to have an economic operator established in the Union, responsible for tasks related to the conformity of that product with EU safety rules. The impact of these provisions on consumer protection are yet to be seen, as the regulation should be subject to evaluation before July 2023.

Having this in mind, we recommend that the impact on consumer protection of new legislation already enacted (e.g., the Regulation on Market Surveillance and Compliance of Products) and proposed (such as the Digital Services Act and the General Product Safety Regulation) is fully assessed before any revisions are made to the PLD and only then reflect on possible measures that could be considered to improve the existing framework. Further, this assessment should specifically look into how any new measure on defective products, if any, could ensure alignment with the E-Commerce Directive general provisions on liability of intermediaries for illegal products and content.

**Risks and Damages**

The consultation raises the possibility to extend the **definition of damages in the PLD** to non-material damage like privacy infringements, psychological harm and cyber vulnerabilities (p. 13-14). We suggest avoiding references to non-material damages as they could potentially lead to waves of compensation claims for producers on illegitimate grounds all while mostly being covered already by existing legislation in the fields of data protection, non-discrimination and freedom of expression. Concepts like psychological harm, which by its nature would be difficult to define and assess, including by a court of law, would increase this risk even more. Looking at the examples of non-tangible damages that are specifically called out, i.e., data loss, privacy infringements, or environmental damages, such claims can already be made under other causes of action (such as fault-based liability). Moreover, a strict liability approach would likely be abused by bad actors looking to game the system given proposed lower evidentiary standards. On the other hand, questions related to privacy rights infringements are already covered by the General Data Protection Regulation (GDPR), which already grants possibility for redress. In any case, it is difficult to see what added value for consumers would come with such a legal change, keeping in mind that the objective of a PLD review is supposed to be simplifying the process for consumers to get compensated.

**Cyber vulnerabilities** should not per se be classified as defects, as these are dynamic risks that can in most instances be mitigated through responsible system configuration to enable remote updates and responsible cyber hygiene practices by consumers. In particular, discovered vulnerabilities in software products can be remedied after the products have been placed on the market via patches developed in a timely manner by the manufacturer.

However, software producers do not fully control in all instances whether updates are installed – oftentimes, it falls to the user to install or accept these updates and in such cases vulnerabilities can either go unnoticed or are not fixed, with users maintaining some level of responsibility for mitigation. The imperative of user responsibility also underscores a particular challenge in the use of existing product testing and certification regimes - which are largely geared toward the assessment of static product safety risks - to fully assess dynamic risks such as cyber vulnerabilities. It is important to educate consumers regarding responsible cyber hygiene practices, so they are aware of the importance of updating systems in those instances where automated remote updates are unavailable.

**Circular Economy**

The question in page 14 of the questionnaire asks if changes to a product made after it is placed in the market should be covered by the PLD. ITI welcomes this conversation and suggests that liability should be determined on a case-by-case basis taking into account the circumstances of the case, including among others whether the "defect" causing damage was introduced by the relevant remanufacturing/refurbishment/spares activity, or was pre-existing.

**Alleviating the Burden of Proof in the PLD**

Option 2(a) proposed in page 23 of the questionnaire mentions the possibility to alleviate the burden of proof for technically complex products, to facilitate proving the causal link between a defect and the damage. It is unclear here what it is meant by technically complex product and how broad this definition might be. Complexity as such is neither AI-specific nor problematic since the PLD applies to defects of a product, irrespectively of the underlying root causes of the defect. In making such considerations, the Commission should maintain a balanced and innovation-friendly approach. Requiring the disclosure of information to injured parties would in practice shift the burden so that claimants need only allege a hypothetical complaint, and then defendants must "prove a negative" by submitting sufficient technical information to establish the product did not cause the alleged harm. In addition, disclosure of certain types of data to help the injured part prove their claim should not oblige companies to disclose sensitive data that may be protected by trade secrets, intellectual property or privacy rights.

Option 2(b) would allow courts to infer that a product is defective or caused damage under certain circumstances (e.g., when other products in the same production series have already been proven to be defective or the product clearly malfunctioned). This inference could result in the first legally binding decision that a product is defective being applied to all future claims against the product in the same production series. In these cases, producers would have little choice but to settle claims rather than seek a decision on the merits.

Similarly, we urge the Commission to carefully consider any blanket reversal of the burden of proof as proposed in option 3. This tool should only be considered for very specific and limited cases. In fact, a blanket reversal would create an insurmountable burden on defendants to prove a negative, and flies in the face of traditional notions of burden. Legal costs for

companies would likely increase substantially given the likely increase in hypothetical, speculative, and even fraudulent claims. Such unnecessary strain on businesses could have the effect of stifling innovation. Cost and availability of insurance for companies is also likely to be negatively impacted.

**Development Risk Defence**

The consultation (p. 21-22) argues that the development risk defence, i.e., a liability exemption for when the product's lack of safety was not discoverable due to the scientific knowledge at the time of the placement in the market, may be inappropriate for products that are able to adapt while in operation. We strongly caution against the removal of such a mechanism for AI or other software-enabled products. In fact, unknown vulnerabilities can always be present in software, and there exists no deterministic process to test software for defects. Besides, the fact that an AI system learns and adapts does not necessarily pose higher risks. As producers roll out patches and updates throughout the product's lifecycle, the development risk defence should refer to the knowledge that a producer has at the time of the update, in order to better reflect the reality of software development.

## Part II – Liability for AI

An effective and balanced liability regime should foster trust in the use of AI, provide a clear path for redress and adequately compensate victims for damages, while allowing for incremental improvements and innovations that come with placing AI systems on the market. As mentioned above, the PLD has worked well as a technology-neutral instrument to provide for consumer compensation for damages. Given how the key concepts of the AI Act are yet to be established, a revision of the PLD or the introduction of complementary AI-specific liabilities at this stage seems premature. Independent of the development of the AI Act, there is no strong evidence that AI-specific changes to the PLD are warranted. It is also unclear how some of the concepts mentioned in the consultation such as AI systems with "high degree of autonomy" or "opacity" would be defined in practice, thus raising a lot of legal uncertainty with regard to the types of AI systems that would be covered by the rules. Moreover, as the AI Act seeks to introduce new transparency requirements addressing opacity and autonomy of certain high-risk AI systems, it would be useful to assess the impact of these upcoming rules on liability claims before considering new rules. Some of these characteristics are not even AI-specific. Technology-neutrality is thus fundamental to ensure a forward looking and certain liability framework. As per Member States liability rules, a degree of harmonisation of existing rules would generally be a positive outcome to ensure consistency across in the Single Market, benefit legal certainty and increase consumer trust in AI technologies. However, consumer claims and resulting litigations are per se national. As pointed out above, it is more important to avoid new regulatory burdens and unjustifiably spreading liability across the AI supply chain, as it would be unduly burdensome on businesses developing AI-enabled products and services and risks deterring investment and stifling innovation.

**Burden of proof**

The questionnaire (p.34) proposes certain measures to alleviate the burden of proof for claimants when an AI-system is involved. As mentioned above with regard to the proposed adjustments to the burden of proof in p.23 of the consultation, options like requiring disclosure of certain technical information such as log data would imply a shift in the burden of proof that would pose an insurmountable burden on defendants. Further, and as mentioned above, actors in the AI supply chain should not be required to produce confidential information, trade secrets and data protected by privacy laws (e.g., personal data), intellectual property or any other legal rights. This point should be taken into account with regard to the option that would allow courts to infer that the claims are fulfilled if a defendant refuses to disclose certain data/technical information, as there may be legitimate reasons for refusing to provide information, and courts should examine each potential refusal independently. It is also important to consider that many AI providers do not necessarily log input and outputs to and from their models. Maintaining extensive logs would thus be an excessive burden for some developers, especially given how such disclosure requirements would interact with existing requirements under the GDPR on personal identifiable information.

The option to enable courts to infer fault or that a product is defective under the PLD if a provider of an AI system has failed to comply with its obligations under the AI Act may also give rise to uncertainty. Non-compliance with product safety does not necessarily mean that the product has caused a specific consumer harm and the claimant should continuously be required to provide evidence of the causality between defect and harm. In addition, as the AI Act is still under consideration, neither the substantive obligations nor the distribution of responsibility across the supply chain between users, providers, importers, distributors etc. are defined. It is unclear how this measure would apply where there are multiple operators/providers/users of a single AI system, and where there is ambiguity around fault. There is also no clarity on what happens where a person or entity plays a small role in the development, operation, or use of the AI system. Accordingly, there is a risk that actors in the chain may inadvertently (and unknowingly) become liable due to the actions of third parties that use or amend AI systems to which that actor may have contributed, even where that actor is unaware of that use or amendment. It is also unclear how liability would be apportioned where an AI system "learns" as a result of subsequent development by an actor other than the original producer, and the update made ultimately causes, at least in part, damage to a consumer.

The option to eliminate the need to prove defectiveness for claims under the PLD where a product integrating an AI system which "continuously learns and adapts while in operation" causes damage is also disproportionate and may give rise to a wave of compensation claims. Similarly, the reversal of the burden of proof for opaque and autonomous AI systems would also place excessive burden on producers, create ground for hypothetical claims and impact AI innovation. It is unclear how "opaque" or "highly autonomous" AI systems would be construed in practice, and these vague terms would risk capturing a broad range of technologies. As further noted above, in order for a reversal of the burden of proof to be appropriate, the terms "opaque" or "highly autonomous" would need to be clearly and specifically defined. There is also a risk that these definitions would quickly become outdated as the relevant technologies evolve. As such, the reversal of the burden of proof for these

types of systems does not appear to be appropriate. Moreover, this would place an excessive burden on AI developers and users, significantly hampering innovation in the field and affecting the rollout and take up of AI technologies in the EU. Finally, reversing the burden of proof for an undefined subset of systems materially increases the risk of fraudulent claims and increased insurance costs for all businesses that use or develop AI products or services.

**Harmonised Strict Liability**

The questionnaire also suggests that a harmonised strict liability regime separate from the PLD could be extended to certain AI-enabled products or services depending on their risk profile. It is unclear however how the notion of AI risk management, which is useful in the context of the AI Act, interacts with ex-post legislation such as exposure to liability. In many cases the existing liability framework will be easily applied in an AI context and we suggest that the EU maintain a strong presumption against altering it except in response to significant and demonstrable shortcomings. Should a need for future action be identified in areas that involve increased risks for end-users of AI applications, it should be addressed in a sector-specific manner, with new regulation or suggested legislation filling clearly identified gaps and designed to avoid overreach.

In addition, applying the same liability rules to all participants in the AI value chain would risk crippling the diverse ecosystem of AI innovators, experimenters, contributors, and entrepreneurs. Part of what has enabled the AI ecosystem to grow so quickly has been that contributions, many of which are open source, build on each other. For example, a developer can make a small improvement to an AI image recognition framework, and then that same framework can be used in everything from the frivolous to detecting tumors in MRIs. The initial developer may never know if their contribution is used in a high-risk application. But if they are held strictly liable for such contributions, it will deter many of the contributions that have enabled the growth of AI technologies. Complex value chains are not AI-specific and the PLD already covers situations where multiple actors are involved in providing a product. In case of new AI-specific provisions, consistency with these established practices is key.

**Insurance**

Companies have a natural interest in mitigating risks and should not be obliged to take out insurances. This is a commercial decision and is often particularly relevant in areas of high risk. Depending on the individual companies, insurance may be considered as particularly helpful in areas of higher risk, such as for products that may cause serious injuries. In most cases, an insurance limits the costs for the liable person in case of justified claims and insurances usually make it more likely for compensations to be payed.

In the B2B context for example, often there is no insurance for liability claims, but service level agreements that outline the acceptable timeframe to fix a problem, and a liability cap: contracts with business customers would include a limitation of liability provision which limits the amount of damages either party would pay. Issues such as non-material damage or cyber vulnerabilities would lead to a highly increased cap that may be prohibitive for both sides.

Currently, most companies do not have a specific "AI" insurance. Whether or not liability insurance covers AI depends on the type of claim. Changes in legislation could either lead to a gap in coverage (because the insurance contract does not cover the new legislation) and/or to significantly increased premiums, especially if the potential damage is only vaguely defined and the amount unforeseeable. Availability and cost of insurance for companies developing AI and AI-enabled products are likely to increase substantially if certain changes are introduced to the PLD, including particularly if the scope of recoverable damage is extended and strict liability is spread across the AI supply chain. The impact of higher or potentially prohibitive premiums could lead to pricing out smaller developers, which in turn could lead to stifling the development of AI altogether, which relies on a diverse ecosystem as set out above.

**Types of harm**

Compensation rules beyond the PLD are not justified. As regards the question in page 42 about modifying the types of admissible harms for compensation for harm caused by AI under member states national liability rules, we note that, just like in the case of the PLD, it is important that the liability rules remain focused on tangible harms. For the sake of legal certainty, the definition of harm needs to be clear and verifiable. As explained above, the notion of immaterial harm is too vague and may create risks for abuses of the system and backlog in the claims.