December 2022

ITI Comments to the Revision of the Product Liability Directive (PLD): Ensuring a Proportionate Framework for all Actors

Introduction

ITI, the Information Technology Industry Council, welcomes the opportunity to provide input to the European Commission on the revision of the Product Liability Directive (PLD). 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).

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. In previous consultations, our industry has spoken against the need to review the PLD, due to its proven effectiveness[1] and the lack of concrete evidence to date on specific shortcomings of its applicability.[2] The Commission's proposal looks at a variety of issues which will significantly extend the scope of the PLD, including the definition of product, defectiveness, damage, distribution of liability in the supply chain and burden of proof.

This revision will have great impact on the communities of software and AI developers and will significantly increase liability exposure for a variety of actors. For this reason, **it is of the outmost importance to ensure that the framework is balanced and proportionate for all actors**, to pursue consumer protection while at the same time avoid disincentivising innovation. The comments below raise some of the key questions that arise with the extension of strict liability to intangible elements like software and AI.

Potential shortcomings of the extension of the definition of product

The proposals' main changes to the PLD framework in article 4(1) is the expansion of the **definition of product** to include software (embedded and standalone), components, AI systems, and 'related services.' **ITI is concerned about this extension of the definition of product, which fails to take into account the specific characteristics of software.** Unlike software, hardware cannot be fixed remotely, and that justifies a stricter treatment of physical products. At the same time, the tangibility of hardware also creates higher risk of physical harm compared to software, which cannot physically act upon any person or

[1] Also recognised in the Commission's Impact assessment (p.9): https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Product-Liability-Directive-Adapting-liability-rules-to-the-digital-age-circular-economy-and-global-value-chains_en

[2] ITI's views on Adapting Liability Rules to the Digital Age and Artificial Intelligence, https://www.itic.org/documents/europe/1001ITIResponsetoEULiabilityRulesConsultiation.pdf

property. Finally, while bugs are inevitable in software development, hardware malfunctions can be a more infrequent consequence of a permanent design problem or an unforeseen event affecting individual products.

If the EU were to become the first global player to apply strict liability to services and software, especially to the extent that current definitions are left excessively vague and could potentially contemplate a large number of cases which would be difficult to prove, the roll-out and uptake of AI-based technologies would also be hindered. This would impact businesses and start-ups operating in Europe and come 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. **We also note that the Commission is proposing in parallel new rules for non-contractual fault-based liability rules for AI in the AI Liability Directive (AILD).** The combined application of these two regimes risks complicating the regulatory landscape for AI innovators and make the EU AI ecosystem less competitive. Moreover, the AILD specifically anticipates review of inclusion of whether AI systems should be included within a strict liability regime 5 years after commencement of AILD.

Software and AI systems encompass a broad range of technologies that can be deployed in a variety of ways and its characteristics depend strongly on how they are being used. It is important that the proposal clearly defines software, to avoid legal uncertainty with regards to its applicability to digital services, software-as-a-service, AI systems, middleware etc. In addition, a potential application of the concept of defectiveness in the PLD to software and AI should also take into account that 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.

The existing PLD already provides safeguards against defective products, regardless of whether they are equipped with software, but refrains from liability provisions for standalone software which a user downloads and uses. Moreover, national jurisdictions on liability already cover products which include software. There are also substantial existing statutory protections for consumers at EU and national levels for damages caused by software, including the ability to bring fault-based claims in tort and contract law. In addition, the implementation of EU Directives on Digital Content (2019/770 and 771) has provisions related to liability and software updates (applicable to product conformance/consumer contracts). **Therefore, this 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". Indeed, it can be difficult to identify what actually caused a software malfunction and who is the responsible actor. In many cases, cumulative causes may apply. Moreover, a desire to dodge liability may discourage information sharing across the ecosystem and may discourage players along the supply chain from assisting in providing fixes. All of this is to the detriment of the end-user.

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. In fact, 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 strict liability would apply where there are multiple operators/providers/users of a single AI system. 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. **Excessively expanding exposure to strict liability to software and AI developers and others playing an intermediate role in the value chain would be burdensome for the community and ultimately harm its competitiveness.** In relation to components, we support the status quo of the current PLD which focuses on the final manufacturer who has control over its practical use case scenario, rather than the original manufacturer who is not placing it on the market.

The proposal also extends the liability rules to remanufacturers and/or businesses that "substantially modify" products. Meanwhile, the EU is currently developing several initiatives to address current circular economy challenges. New PLD requirements need to be aligned, therefore, with the upcoming right to repair initiative and with existing measures addressing reparability of products (Ecodesign for sustainable product regulation, Battery Regulation, Sale of Goods Directive etc.). In addition, integration, configuration, or optimisation services alone should not be treated automatically as substantial modification and subject to strict liability. We therefore recommend clarifying how the "substantial modification" of a product will work in the context of EU repairability legislations and the thresholds that constitute a "substantial modification". **Original Equipment Manufacturers (OEMs) should not be held liable for self-repair or repair done through non-certified repair shops**.

We support the exclusion of open-source software in recital 13, **and we call to specifically add this exclusion directly into the article of the text in addition to the recital.** However, participants in the open-source ecosystem could still be exposed to strict liability in the event that a software is commercialised. 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 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. **We therefore call to extend this exclusion to all open-source software.**

In addition, the proposal brings “related services” in scope, although recital 15 expressly states that “this Directive should not apply to services”. **The definition of "related services" is very broad and could cover many digital services interacting with technology products** (e.g., services delivered through apps). The inclusion of related services in the PLD scope also results in an inconsistent liability regime if providing a service digitally (e.g., on an app) leads to strict liability, whereas providing the same service in a non-digital manner is not in the scope of the PLD.

Clarify the scope of the damages

Strict liability is for cases of direct, tangible and severe harm for individuals, such as personal injury or damage to property. **It is not appropriate for strict liability to be extended to (i) psychological harm or (ii) data loss/corruption**, due to the challenges caused by remoteness of loss, quantification of damages and causation. In the case of software, such damages are typically not foreseeable at the time of development and can be potentially unlimited. This is made worse by the lack of a clear definition of (i) medically recognised harm to psychological health, (ii) data, (iii) data loss and (iv) data corruption. In addition, it is unclear how the inclusion of ‘loss or corruption of data that is not used exclusively for professional purposes’ overlaps with existing regulation and representative actions available under other laws such as GDPR for data breach or similar breaches of obligations thereunder. Inclusion in PLD creates a risk of confusion and multiple claims for the same loss.

The definition of damages in article 2(6)(b) of the proposal also extends the scope of the PLD to damage occurred to property that has a ‘mixed’ personal-professional use. Specifically, point 2(6)(b)(iii) excludes damages to property used exclusively for professional purposes and point 2(6)(c) limits the damages to corruption of data not exclusively used for professional purposes. **We encourage EU lawmakers to better clarify this notion as in many cases it will be unclear whether damage to products and services that have a mixed use would be included in scope.** For example, it is not clear whether it includes damages to products that are only occasionally used in a personal use, or products that are not expected to be used for personal use. For this reason, we suggest clarifying that the PLD should only apply to damages to products or corruption of data not ‘primarily’ used for professional purposes.

We also welcome the exclusion in the memorandum of the proposal (page 6) of other types of harm, such as privacy or discrimination, which are already covered in other legislations. For legal clarity, the text should explicitly exclude discrimination, privacy infringements or discrimination as possible causes of harms under the PLD.

Clarify how the traditional concept of defectiveness can apply to intangible elements

The PLD revision defines in article 6 defectiveness as a failure to provide the safety which the public at large is entitled to expect. A variety of circumstances are then listed in points (a-h) which should be taken into account when assessing defectiveness. **The extension of the scope of the PLD to intangible elements like software and AI implies a different conception of defectiveness under the PLD. In fact, it is difficult to apply traditional strict liability defect types (i.e., manufacturing, design, and warning) to AI and software.** For example, manufacturing defect theories are inherently inapplicable to software. Code is infinitely replicable with perfect fidelity, so production defects really do not occur in a software context. Design defects on the other hand will be very difficult to assess in the AI context. These claims typically rely on foreseeability of potential harm that could have been avoided or reduced by adopting a reasonable alternative design. Some harms might be foreseeable depending on the use case (e.g., a pedestrian collision for self-driving cars). But for example for general purpose AI, foreseeability is nearly impossible. The state of the art is also very difficult to define in the AI context—further complicating foreseeability and the link with reasonable alternative designs. Finally, failure to warn defects are inherently subjective and typically use negligence principles anyway. So strict liability for warnings and instructions effectively becomes a negligence analysis.

Article 6(1)(c) expands the notion of defectiveness to the "*effect on the product of any ability to continue to learn after deployment".* However, it should be clarified how this factor weighs for/against liability of the developer when that learning happens outside of their control. In addition, the “specific expectations of the end-users for whom the product is intended” (Article 6 (1) (h)) remains an unclear and subjective element that does not present any reasonable standard of control and would need to be clarified as well.

Article 6(1)(f) also includes safety-relevant cybersecurity requirements among the circumstances to take into account when assessing defectiveness. **It is not clear here if cyber vulnerabilities would be considered as a defect.** This should not be the case 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. Applying strict liability will stifle cybersecurity professionals and likely lead to delays in launching products out of concern that some unknown, and potentially unknowable, vulnerability exists. 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 or even not permissible. For example, remote updates are problematic under the Sale of Goods Directive EU 2019/771, since the user should be able to decide in every case whether they want to install updates or not (cf. recital 30: “The consumer should remain free to choose whether to install the updates provided”.)

Adequately protect sensitive information subject to disclosure orders

Article 8 (2-4) contains certain protections for confidential information and trade secrets from disclosure in liability proceedings by injured claimants**. Paragraphs 2-3 in particular are rather vague and limit disclosure to what is "necessary and proportionate",** which must consider "the legitimate interests of all parties". Paragraph 4 provides for protective measures when confidential information/trade secrets are referred to in legal proceedings, which can either be invoked by the courts, or upon a reasoned request by a party.

The risk we see is that the practical application of the provisions under article 8 during the course of proceedings is subject to changes in different national courts and under different laws, which creates a significant degree of uncertainty as notionally high-level concepts such as proportionality and legitimate interest, as well as courts willingness to apply protective measures on their own initiative, are not especially well harmonised across Member States. In addition, we note that the threshold for obtaining documentation is very low, while the scope of documentation that can be obtained is wide.

The drafting of the article should thus be tightened to better protect trade secrets in product liability proceedings. For example, the article could be clarified to state that, when determining whether to order the defendant to disclose information which is protectable as confidential information and/or trade secrets within the meaning of Article 2, point 1, of The Trade Secrets Directive (EU) 2016/943, national courts must consider *inter alia* that the disclosure of such information is "relevant and necessary" for the claimant to demonstrate in the course of the legal proceedings that the product is defective. Access request should remain limited to information required to assess whether the product was defective, who was the liable actor (manufacturer, repairer, …) or the causal link. This would ensure higher standards and more detailed consideration for disclosure than merely whether it is "proportionate".

Ensuring proportionate adjustments to the burden of proof

Article 9 lays out several presumptions that courts can use to alleviate the burden of proof on claimants. According to article 9(2), the defectiveness of the product can be presumed if the defendant failed to disclosed evidence as per article 8; if the claimant proves that the defendant did not comply with mandatory safety requirements meant to prevent the damage that has occurred; or if the malfunction is obvious. **However, it is not clear why a refusal to comply with a disclosure order should trigger a presumption of defectiveness, instead of being penalized in the same way as any other refusal to comply with a disclosure order.** It is also important to consider that there may be legitimate reasons for refusing to provide information. In addition, in the case of AI, 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.

At the same time, 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.

Article 9(2)(c) also provides a presumption of defectiveness when an "obvious malfunction" of the product caused the damage. **However, it is unclear what the term "obvious malfunction" will cover.** If the threshold for an "obvious malfunction" is lower than for "defect" then this would effectively make strict liability even easier to engage.

Article 9(4) also empowers courts to presume the defectiveness of the product, the causal link between the defectiveness and the damage or both when claimants face excessive difficulties due to the technical and scientific complexity of the product. Recital 34 clarifies the definition of technical complexity, by referencing complex technology like Machine Learning, complex functioning like Medical Devices or complexity in the nature of the causal link (for example when the claimant would have to 'explain the inner workings of an AI system'). **Depending on how the broad notions of complexity will be construed, this presumption could apply to a broad range of technologies, including all AI systems, which would be disproportionate.** We urge policymakers to better characterize these notions, to ensure that the presumptions can apply only in cases where it would be objectively impossible for the claimant to prove the defectiveness of the product or the causal link between the defectiveness or the damage. Without clear thresholds, this alleviation of the burden of proof could lead to tremendous litigation and could also significantly hinder companies from bringing products to the EU market.

In the case of AI for example, the notions of explainability and interpretability of AI are still subject to a debate and there is no consensus over their definitions. A helpful conceptual distinction may be viewing explainability as explaining the outputs of an AI model in a way that humans understand, focused more on the how, and interpretability as allowing humans to understand the inputs and outputs of the AI model, focusing more on the cause of the decision.[3] It is however unclear from the proposal what characteristics of AI would contribute to the designation of a specific AI system as complex, and policymakers should seek to clarify this aspect in the text.

At the same time, while recital 34 refers to 'having to explain the inner workings of an AI system,' **different AI models can have different levels of explainability, some of which are relatively easy, and some more complex.** For example, simpler models like decision trees are considered inherently interpretable due to their simple structure. On the other hand, more complex AI models require post-hoc explanation models that construct explanations from properties of the model. To avoid a blanket classification of all AI technology as 'complex' and therefore non-explainable, lawmakers should better reflect these nuances and restrict the designation of complexity.

Liability exemptions

[3] ITI, Policy principles for enabling transparency in AI systems, 2022: https://www.itic.org/documents/artificial-intelligence/ITIsPolicyPrinciplesforEnablingTransparencyofAISystems2022.pdf

Article 10 includes a variety of scenarios that would represent an exemption from liability, including where the defectiveness did not exist at the moment the product was placed in the market (art. 10(1)(c)). Article 10(2) creates a derogation from the exemptions in article 10(1)(c) in cases where the defectiveness of the product is caused by software or software updates or the lack of software updates or upgrades, provided this is within the manufacturer's control. **We support the exemption of liability when the failure to provide the updates or upgrades is beyond the manufacturer's control.** To increase clarity, the text should however also explicitly exclude software versions that are no longer supported by the developer.

Software updates are essential for promoting security, innovation and consumer welfare, including safe use. Failure to install updates, including important security updates, is widely recognized as a major contributor to the insecurity of and/or safety concerns associated with many consumer devices. **Elements related to user responsibility need to be considered when it comes to software updates and upgrades.** 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.

The exemption for manufacturers of defective components where the defect is from the product manufacturer's design or instructions (Article 10 (1) (f)) should also be expanded to include scenarios where the product manufacturer uses the component in way the component manufacturer has explicitly said is prohibited and/or is not an intended use of the component. In addition, changes to the intended purpose of any software, the objective characteristics and the properties of the product, or specific requirements of the group of users for whom the product is intended (the criteria set forth in Recital 22) by another entity should be added as an additional exception.

Removal of the thresholds

The combination of the removal of minimum (€500) and maximum (€70m) thresholds with the new presumptions, types of damage and types of products (and therefore defects in these further product types) upsets the careful balance of the current Directive. This overall perspective needs to be addressed when weighing the individual extensions being proposed. The reasoning for having such thresholds remains true today; **a minimum threshold prevents frivolous claims and maintains the back-stop nature of the regime**, **while an upper maximum allows for insurable risks.** These figures should be subject to maximum harmonisation to address issues the Commission identifies with the current divergence across member states.

Clarifications to the distribution of liability in the supply chain

We welcome the recognition that economic operators which have no power over the manufacturing process (e.g., online marketplaces, retailers) should not be considered as having the primary liability in cases of damage caused by defective products unless no other party in the EU can be identified within 1 month. This should also be the case for fulfilment service providers, who should not be placed in a worse position than retailers. The proposal should remove article 7.3 and instead refer to article 7.5 as the marketplace provision in article 7.6 does. It would be disproportionate to hold marketplaces liable as they are often not in contact with the producers or the importers, and would negate the purpose of online marketplaces.

The proposal includes new reference to the Responsible Person concept (from the Market Surveillance Regulation and the draft GPSR) to take liability for harm caused by defects where there is no EU-based manufacturer or importer. This is a proportionate allocation of liability, but **the RSP concept must be made meaningful to support inclusion in this framework and the risks they take on must be insurable.** The availability of insurance is closely connected to retaining and strengthening the liability thresholds in particular.

The first step to enhancing the RSP is to make them "reliable" by professionalising the role of an Authorized Representatives. We recommend establishing a minimum set of criteria for Authorized Representatives, accredited as the RSP, as an entity who is both legitimate (i.e., remove the ability to assign "anyone" to act as an Authorized Representative) and possesses sufficient understanding of product compliance requirements to be responsible and therefore play a meaningful role in minimising risk of harm from defects along with taking liability for them. The European Commission already has mechanisms for accrediting Notified Bodies,[4] and such a mechanism could be used as a reference to create an accreditation program for RSPs.[5] Similar for notified bodies, it is essential that the RSP has access to personnel with sufficient and relevant knowledge and experience to be able to collect more compliance information, such as test reports and safety signals. They should also possess the necessary skills and expertise to be able to verify those documents and ensure they are not fraudulent; if documents are found to be fraudulent, RSPs should be able to provide information to market surveillance authorities to enable investigation of bad actors.

The next step is to also enable verification of RSP so that marketplaces, fulfilment service providers, consumers, and regulators can confirm the status of an RSP. An RSP "Registration Database" for Authorised Representatives (where there is no EU based manufacturer or importer) should be created for this purpose, which will enable interested parties to view all relevant and necessary information efficiently and at scale. Such a publicly accessible mechanism helps to incentivise a high standard for the RSP. At present, a rogue actor wishing to appoint a phantom RSP can easily create fake contact details, which presents challenges to businesses or market surveillance authorities to confirm the presence of a valid RSP. Having a centralised database would mean that this system of verification would be much more robust and also give the option of automating this verification.

Limitation period

The limitation period for software in Article 14 should correspond to the warranty period for digital content in the Digital Content Directive. A limitation period of 10 years is not

[4] P75-8 Blue Guide https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016XC0726(02)&from=DE.

[5] Section 5.2.2. of the 'Blue Guide' on the implementation of EU products rules 2016 (2016/C 272/01) which outlines the roles and responsibilities of notified bodies.

practicable in view of the implicit software update requirements in the PLD and the life expectancy for software.

In addition, a clarification would be welcome that releasing a software update does not constitute a new placing on the market with regards to the limitation period. Otherwise, the limitation period could extend indefinitely for software, given the implicit requirement on producers to provide continuing software updates.

***