BSA RECOMMENDATIONS ON THE DRAFT EU PRODUCT LIABILITY DIRECTIVE

MARCH 2023

SUMMARY

BSA | The Software Alliance ("BSA")[1] is the leading advocate for the global software industry before governments and in the international marketplace. Our members[2] are at the forefront of software-enabled innovation that is fueling global economic growth and digital transformation by helping enterprises in every sector of the economy operate more efficiently, securely and in a privacy-protective way. BSA's members are enterprise software companies that offer technology services that other organizations use – such as cloud storage services, customer relationship management software, and workplace collaboration software – to make their own operations more efficient, innovative, and successful.

BSA welcomes the EU Commission's objective of the revision of the Product Liability Directive (PLD) to ensure the functioning of the internal market, free movement of goods, undistorted competition between market operators, and a high level of protection of consumers' health and property. To that end, it is important for the new liability rules to respect the differences of products and services and the business-to-business supply chains, which provide for a clear and effective allocation of liability. Overall, it is important that any new liability regime would be based on the actual need and identified problems.

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry. Its members are among the world's most innovative companies, creating software solutions that help businesses of all sizes in every part of the economy to modernize and grow. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy. Follow BSA Twitter @BSAnews.

[2] BSA's members include: Adobe, Akamai, Alteryx, Atlassian, Autodesk, Bentley Systems, BlackBerry, Box, Cisco, Cloudflare, CNC/Mastercam, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intuit, Juniper Networks, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Prokon, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trellix, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

BSA submits six recommendations for consideration by the EU co-legislators to ensure a balanced and effective product liability regime:

1. Traditional product liability rules should not be simply extended to standalone software that is more akin to a service.
2. Initial liability should lie with the entity best placed to mitigate the harm.
3. If the product has incorporated components, initial liability should be tied to a manufacturer of a final product, which has decided how to incorporate the components.
4. The concept of "defectiveness" should be clarified.
5. There should be no overlap with other EU legislation and other liability regimes.
6. A balanced approach should be ensured when defining liability.

1. TRADITIONAL PRODUCT LIABILITY RULES SHOULD NOT BE SIMPLY EXTENDED TO STANDALONE SOFTWARE THAT IS MORE AKIN TO A SERVICE.

The draft PLD seeks to classify standalone software as a product. However, modern software can have many attributes that are normally associated with a service and would therefore be ill-suited to the product-focused liability regime of the draft PLD. Introducing strict liability for standalone software could extend liability to developers that could not reasonably be expected to bear responsibility for situations beyond their control. Standalone software can be integrated and deployed in an almost unlimited number of scenarios and for a wide range of uses. The draft PLD provisions, which are designed for products, could result in considerable challenges for standalone software used inappropriately.

The draft PLD should exclude standalone software, especially software supplied by so-called "as-a-service" models, from its scope, given its fundamentally different nature from physical products. Strict liability regime for standalone software could have a detrimental impact on software development and innovation in Europe. Software developers could be discouraged from innovating, leading to less innovative features, reduced performance, and trends towards more basic functionalities.

However, if standalone software were to be included in the scope of product liability rules, the proposal should:

- reserve strict liability regime to extreme circumstances involving abnormally dangerous activities that impose substantial risks to others, therefore for cases in which software may present **material risks of severe harm**; and
- avoid overlapping and inconsistent standards especially for the **artificial intelligence (AI) systems**, therefore the AI systems should be excluded from the scope of the draft PLD altogether. Liability for AI systems should instead be regulated by the AI Liability Directive,

which specifically anticipates a review of AI Liability five years after its entry into force and is directly linked to the AI Act.

In addition, for years, the European Commission, in negotiations with its trading partners, has taken the position that standalone software should not be treated as a "product" within the meaning of the WTO General Agreement on Tariffs and Trade (GATT). Accordingly, the Commission has often taken the position that the provision of software, especially electronically, should be treated as a service under the General Agreement on Trade in Services. This has enabled the Commission to maintain the position that Member States' local content requirements and similar measures to promote European culture are permissible under WTO rules, since in that case the GATT's "national treatment" principle arguably does not apply. If the EU were to classify standalone software as a "product" under the PLD, this could make it difficult to maintain the position that software should not be treated as a product under the WTO rules.

Moreover, the revised PLD should be consistent with current EU legislation addressing product safety such as the recently adopted General Product Safety Regulation, which will be the baseline to address product's defectiveness in the EU market and which does not consider standalone software as a product.

2. INITIAL LIABILITY SHOULD LIE WITH THE ENTITY BEST PLACED TO MITIGATE THE HARM.

To ensure that the liability would be allocated with the parties, who actually control software functionality and direct how it will be used, the draft PLD should introduce definitions of "**software developer**" and "**software deployer**".

In contrast to products, a developed standalone software usually has many operating possibilities and different available settings, which are created by the software developer, and which, based on the decision of the software deployer, can be put into use in many different ways. This is a decision of software deployer, not software developer. Enterprise software developers create innovative, tailored, or customizable solutions for their business clients – software deployers – who then take decisions on the deployment of software with a concrete functionality and characteristics. It is important for business-to-business (B2B) **parties to be able to keep their best practices** and place liability with the party that is best placed to mitigate the harm through contractual/licensing agreements. This would also guarantee an effective compensation for consumers, allowing consumers to claim liability from the party that takes decisions on the use and manages the risks. Later, software deployers could seek compensation from software developers under their B2B agreements.

All in all, in order to maintain clarity for all service providers involved, keep responsibility with a B2B party that takes decisions and ensure effective compensation for consumers, it is important that **software deployers remain initially responsible for the purposes of PLD**, not software developers.

3. IF A PRODUCT HAS INCORPORATED COMPOENTS, INITIAL LIABILITY SHOULD BE TIED TO A MANUFACTURER OF A FINAL PRODUCT, WHICH HAS DECIDED HOW TO INCORPORATE THE COMPONENTS.

Software can often be an integral part of a product, have multiple parties involved in its supply chain and have many operating possibilities and different available settings. These settings, in turn can be configurated based on the decision of the product manufacturer and be put into use (or not) when placing the product on the market. One product can have several components/software elements and tools integrated which may be produced by different B2B software developers. Often the development of one single software component involves a **complex B2B supply chain**.

In B2B relations, the allocation of risks and responsibility is often one part of the contractual agreement/licensing between two or more business entities, and it reflects the complexities of supply chain. The current PLD provides a **clear path for consumers to seek redress from a manufacturer of a final consumer facing product, and liability is in turn normally addressed contractually between the B2B parties that are upstream in the product supply chain**.

These longstanding contractual B2B relations should not be undermined and the consumer should not be required to seek redress from upstream parties in a supply chain, looking for the manufacturers of different components of a product. Doing so would place an unreasonable burden on consumers, who may have no knowledge of how to identify the correct entity that may be responsible along a supply chain. It is important that Article 13 of the draft PLD **allows the best B2B practices to continue**. Business entities have relied on contractual terms to allocate responsibilities and liabilities, and this system has proven to be effective and innovation-friendly, as it allows for the necessary flexibility along complex supply chains.

As the Explanatory Memorandum of the draft PLD explains, the legislative changes aim to ensure high level of consumer protection no matter whether the defective product is tangible or digital or the defect comes from the integrated component, ensuring consumers' right to compensation for damage suffered. We believe that the best way to ensure that is to maintain the **initial liability to a manufacturer of a final product** not to its components' manufacturers.

4. THE CONCEPT OF “DEFECTIVENESS” SHOULD BE CLARIFIED.

Under the draft PLD, defectiveness is associated with the lack of safety which the public at large is entitled to expect. It is unclear, however, how the defectiveness characteristics will apply to software and AI systems. Defectiveness of a product is presumed when the product does not comply with mandatory safety requirements laid down in EU law. However, for many digital technologies there are no sector specific rules and regulations in place with some sector specific rules currently under negotiation (such as the Artificial Intelligence Act or the Cyber Resilience Act). As the defectiveness of a product is the ground for liability, it should be defined as clearly as possible and leave as little room for ambiguity as possible.

The draft PLD does not provide for clarity on **which exact legal obligations**, if not complied with, would bring strict liability for software developers under the draft PLD. Also, it should be made clear **which legal acts** set mandatory safety requirements for emerging technology and, in any case, **product testing and certification** should be explicitly out of the scope of the draft PLD. The draft PLD also 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 against liability for the developer when that learning happens outside of their control.

The draft PLD presumptions on liability tied to software not meeting safety-relevant cybersecurity obligations bring in ambiguity. A **product should not be considered defective as a result of issues related to cybersecurity requirements.** Cybersecurity is an ongoing struggle against existing and evolving threats and cybersecurity professionals constantly strive to stop malicious actors. Launching products and updates at a fast rate is essential to keep up with actors that are constantly looking for new ways to find issues. 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.

Under the current PLD, manufacturers are exempt from liability if defectiveness did not exist when the product was placed on the market, put into service or made available on the market. Yet, the draft PLD narrows down this rule and holds manufactures liable for the defectiveness, even if it did not exist when the product was placed on the market, if the defectiveness is due to: (a) a related service; (b) software, including software updates or upgrades; or (c) the lack of software updates or upgrades necessary to maintain safety (provided that it is within the manufacturer’s control).These changes would create significant problems in practice.

First, the definition of "**manufacturers' control**" is unclear and potentially exceptionally broad. Control is defined through "authorization", which could be too broadly interpreted. A software developer creating a link or means for integrating with a third-party component should not be deemed to authorize the integration of that component and thereby be liable for damage caused by that component. The term “authorization” should be replaced with a stronger verb, like "instruct"

or at least "explicitly authorize". Second, the reference to "**related service**" is problematic from the perspective of products that have "connectors" that enable integration with third party apps, services and data. For that reason, the subpart (a) of Article 10 paragraph 2 on related services should be eliminated or clarified so that a manufacturer developing or making available a connector is not considered providing an implicit "authorization" for a related service. Third, the draft PLD should be clarified to exclude **software versions that are no longer supported** by the developer from its scope.

The draft PLD alleviates the burden of proof for technically complex products to facilitate proving the causal link between a defect and damage. There is, however, no clarity on what could constitute **"technically complex" products**. Complexity is neither AI-specific nor problematic since the PLD applies to defects of a product, irrespective of the underlying root causes of the defect. Further clarity must be introduced on the necessary threshold to exempt claimants to prove the causal link between defect and damage in case of technically complex products.

5. THERE SHOULD BE NO OVERLAP WITH OTHER EU LEGISLATION AND OTHER LIABILITY REGIMES.

It is important that duplication of legislation is minimized and that any liability reform responds to actual and clearly identified barriers to consumer redress for defective products. To that end, it is needed to ensure that the draft PLD rules do not compete or overlap with the liability rules under other legal acts, such as the General Data Protection Regulation (GDPR) or the draft AI Liability Directive.

The draft PLD introduces some new categories of damage which subjects manufacturers to liability for "loss or corruption of data that is not used exclusively for professional purposes", instead of relying on existing regulation and legal remedies available in other legislations such as the GDPR (i.e. data breaches and related obligations are already governed there for personal data). Inclusion of "loss or corruption of data" in the draft PLD creates a competing and overlapping liability system and risks confusion and, possibly, multiple claims for the same loss or, at the very least, it would make it more difficult for claimants and defendants to decide under which regime a claim should be made. If the intention is to cover non-personal data, then **personal data should be excluded from the remit of compensable damage under the draft PLD**. Creation of an overlapping liability regime for loss or corruption of data would decrease clarity for both, consumers and businesses. We would therefore oppose the inclusion of the loss or corruption of data into the scope of damage recognized by the draft PLD. Especially when there is not enough clarity as to what could constitute "material damages" linked to loss or corruption of data and what threshold would need to be triggered (e.g., financial) to claim compensation for damage.

At the same time, the draft PLD should **not create overlapping liability regime for artificial intelligence**, which should be regulated under the draft AI Liability Directive. The draft AI Liability Directive is directly linked to the draft AI Act, and would best serve to address the specific concerns brought about by AI, especially as the EU works towards establishing a risk-based approach for AI. Additionally, the draft AI Liability Directive provides for a review clause five years after the entry into force, thus providing the necessary flexibility for the co-legislators to address possible challenges that may have arisen in the meantime, and at the same time assess the actual functioning of the draft PLD, AI Liability Directive and AI Act.

However, the draft PLD suggests to already provide for no-fault liability for AI. Therefore, in certain cases, both the PLD and AI Liability Directive liability regimes might be triggered, thus creating significant legal uncertainty for AI developers and deployers. To avoid this and not to overburden innovation, AI systems should be excluded from the scope of the draft PLD and AI liability should be regulated in the draft AI Liability Directive.

6. A BALANCED APPROACH SHOULD BE ENSURED WHEN DEFINING LIABILITY.

- **Disclosure of evidence.** The threshold for ordering such disclosures remains very low. It should be clarified to better protect trade secrets and avoid diverging legal interpretations among Member States. It 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 under the Trade Secrets Directive, national courts must consider 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.

- **Limitation period.** The limitation period of 10 years does not grasp the realities of software development or AI applications. Products can have widely varying product lifecycles and requiring support for long periods can remain very challenging for manufacturers. Under the draft PLD, software developers would have to provide updates for a period of 10 years which does not reflect the duration of software programs. The liability limitation period for products including software should be aligned with the Digital Content Directive and Cybersecurity Resilience Act proposal in order to reflect the realities of software development and keep consistencies between these two legislations.

- **Psychological harm.** With regard to psychological harm, further clarity is needed on what could constitute material damages and what thresholds (e. g., financial) would need to be met to claim compensation for damage to psychological harm. "Medically recognized" should be defined to include what claimants must prove (i.e. diagnosis by any medical professional and/or defined categories of conditions or standards) to claim such damage.

******

For further information, please contact:
Irma Gudziunaite, Director, Policy – EMEA
irmag@bsa.org