

BSA submission to the public consultation on the Digital Services Act

Brussels, 08 September 2020

Chapter I, Section 2, question 8

Question: What would be appropriate and proportionate measures that digital services acting as online intermediaries, other than online platforms, should take – e.g. other types of hosting services, such as web hosts, or services deeper in the Internet stack, like cloud infrastructure services, content distribution services, DNS services, etc.? (*maximum 5,000 characters*)

Answer: ***It will be important for any future legislation aiming to tackle illegal content online to prioritize strengthening consumer protection and user safety standards, while preserving the ability for digital businesses to grow and innovate. To achieve this objective, differentiating between business-to-consumer (B2C) and business-to-business (B2B) services will be essential, and the proposal for a Digital Services Act should have a precise scope, accounting for the existing different business models and practices, roles in the online ecosystem, and responsibilities when it comes to illegal content. As an example, the differentiation between content curation services and the technical services which provide the backend infrastructure to deliver this content without having control over it, should also be considered.***

Chapter I, Section 2, question 23

Question: Are there other points you would like to raise? (*maximum 3,000 characters*)

Answer: ***Regarding the “Know Your Business Customer” provision, we would recommend addressing any existing shortcomings through a tailored approach. BSA strongly supports rules that will protect consumers by preventing dishonest businesses selling illegal products online, but such rules should avoid applying inappropriate constraints on business-to-business services. Setting stronger consumer protection rules should first take into account the role of digital services that are an active party in the provision of a business-to-consumer good or service, while balancing the need to safeguard the smoothness and speed of online business operations. As an example, digital services which are directed primarily at consumers, which act as the intermediary between the trader and the consumer or which provide the trading interface/platform for the online sale of consumer goods, could be considered as relevant parties.***

On the other hand, the provision of core services to regulated sectors such as operators of essential services entirely depends on the ability to provide robust cloud solutions that are neither designed nor intended to/ directed at consumers. Moreover, enterprise cloud-based solutions are largely made available on a “Pay as You Go” principle, contributing to the success of the cloud. Enterprise software suppliers possess a variety of due diligence tools (i.e. contractual obligations in their service contracts) that set strong safeguards, in addition to comprehensive anti-piracy programs and technical safeguards. Additional and disproportionate requirements may not only raise privacy and/ or business confidentiality concerns, but it could discourage companies, particularly SMEs and start-ups, from moving to the cloud. Consequently, the DSA should seek to clarify which consumer-facing services, sectors or activities require specific transparency criteria with the objective of strengthening consumer protection standards and exclude B2B services which provide the backend infrastructure or that store content or data as part of a service provided to a company or another entity other than a natural person.

Chapter II, question 1

Question: How important is the harmonised liability exemption for users’ illegal activities or information for the development of your company? (please rate from 1 star (not important) to 5 stars (very important))

Answer: **5 stars out of 5**

Chapter II, question 2

Question: The liability regime for online intermediaries is primarily established in the E-Commerce Directive, which distinguishes between different types of services: so called ‘mere conduits’, ‘caching services’, and ‘hosting services’. In your understanding, are these categories sufficiently clear and complete for characterising and regulating today’s digital intermediary services? Please explain. (maximum 5,000 characters)

Answer: ***We are of the view that the key principles of liability enshrined in the e-commerce directive should be maintained. As a general principle to be upheld from the directive, liability should fall on the entity best positioned to mitigate the risk. In terms of practical implementation, the framework has worked well since its entry into force. Notwithstanding the above, it could be complemented and supported by reflections on specific business models or types of services, for example further clarifying conditions for liability exemptions under the “hosting services” category (i.e. differentiating, where it is relevant, business-to-consumer vs. business-to-business practices) or, where relevant and appropriate, further harmonization of existing definitions. Finally, a liability exemption for purely technical services or services that are not dealing with content curation should also be considered.***

Chapter II, question 3

Question: Are there elements that require further legal clarification? (*maximum 5,000 characters*)

Answer: ***Better elaboration on the types of services that fall into the purely technical services area could be useful, in particular webhosts, enterprise cloud and DNS services, as well as technical services which provide the backend infrastructure to deliver content without having control over it, should not be included in the scope.***

Chapter II, question 4

Question: Does the current legal framework dis-incentivize service providers to take proactive measures against illegal activities? If yes, please provide your view on how disincentives could be corrected. (*maximum 5,000 characters*)

Answer: ***Not to our knowledge. The general appreciation of the current legal regime is that it does neither impede nor disincentivize service providers from deploying proactive and non-compulsory measures against illegal activities online.***

Chapter II, question 5

Question: Do you think that the concept characterising intermediary service providers as playing a role of a 'mere technical, automatic and passive nature' in the transmission of information (recital 42 of the E-Commerce Directive) is sufficiently clear and still valid? Please explain. (*maximum 5,000 characters*)

Answer: ***We believe that the current definitions of active and passive, including in the hosting category, are valid and they remain pertinent in the current ecosystem. However and as specified in our answer to question 2 (above), additional clarification and where appropriate further harmonization of existing definitions would nonetheless be welcome.***

Chapter II, question 6

Question: The E-commerce Directive also prohibits Member States from imposing on intermediary service providers general monitoring obligations or obligations to seek facts or circumstances of illegal activities conducted on their service by their users. In your view, is this approach, balancing risks to different rights and policy objectives, still appropriate today? Is there further clarity needed as to the parameters for 'general monitoring obligations'? Please explain. (*maximum 5,000 characters*)

Answer: ***We believe that the existing approach remains highly relevant in the current ecosystem. From a harmonization perspective and in the context of the provision of cross-border services within the EU, it is paramount to ensure that general monitoring obligations are not being introduced nationally when the Digital Services Act is transposed.***

Chapter II, question 7

Question: Do you see any other points where an upgrade may be needed for the liability regime of digital services acting as intermediaries? (maximum 5,000 characters)

Answer: ***[Do BSA members have any suggestion for input?]***

Chapter III, section 'Main relevant criteria', question 3

Question: How could different criteria be combined to accurately identify large online platform companies with gatekeeper role? (maximum 3,000 characters)

Answer: ***The identification and regulation of gatekeepers should focus on well-thought market-relevant criteria. For instance, the size or revenue of an organization should not be taken for decisive benchmarks as they would not necessarily imply a gatekeeper role or a dominant position within the sector. Notwithstanding the above, BSA would support defining a set of blacklisted unfair commercial practices such as the practice of intentionally refusing, controlling, or delaying access to services, or raising illicit barriers to entry for competitors.***