ITI Promoting Innovation Worldwide

7 September 2020

The EU Digital Services Act: ITI Views on the Public Consultation

The Information Technology Industry Council (ITI) appreciates the opportunity to comment on the European Commission public consultation on the Digital Services Act Package. In addition to this submission, we are also sharing separate comments on the New Competition Tool consultation that is running in parallel to this exercise.

ITI is the global voice of the tech industry. Our member companies include leading innovation companies with worldwide value chains and active through all the segments of the technology sector. We therefore understand and recognise our shared responsibility to maintain a safe, inclusive, and innovative online environment, and support the commitment of policymakers to safeguarding citizens from harmful and illegal content online and maintain a well-functioning, competitive online ecosystem. It is paramount that all relevant players work together to ensure that the internet has sufficient protections for users, smaller businesses and brands.

As we noted in our views for a framework for digital services, and the 30 June submission to the DSA Inception Impact Assessments (IIAs), online intermediaries play a foundational role in driving innovation and growth in the economy, supporting the smooth operation of digital supply chains and creating market opportunities and access for businesses of all sizes. We appreciate that policymakers around the world are grappling with real challenges caused by the scale, speed, and complexity of various types of platforms and the roles they play.

As the notion of platform refers to very different business models, policymakers should consider the role that specific companies play in the markets they operate in, the value they create, their relationship to customers and competitors, and the possible alternatives. Grasping differences in business models and user interaction across digital platforms is key to gauging potential non-competitive conduct and properly addressing any challenges. The goal should be to **ensure market access for innovative challengers, ensure consumer welfare and economic efficiency, and focus on resolving proven market failures by targeting the appropriate actions.**

Proportionate instruments that result in a consistent policy approach and fair competition should be considered wherever necessary. Still, remedies should focus on the specific situation, and be preceded by a consideration of whether other, less radical alternative approaches would be effective. It would be difficult to enact a one-size-fits-all approach across all types situations and business models. Artificially constraining the size of a company or network may appear to increase competition, but it could also reduce consumer welfare. Policymakers should consider how to ensure that new market entrants are able to succeed, while not imposing rigid rules that disrupt the consumer experience or value that they receive from a platform.

We support the goals of the Digital Services Act to increase legal certainty, clarify roles, and define responsibilities for actors in the online context, i.a. by reviewing and bringing more clarity to the framework. We are committed to working with the European Institutions to forge a balanced framework preserving the current limited intermediaries' liability rules and rights of third parties, for a

healthy online ecosystem, while clarifying where more legal certainty would be helpful. We support the European Commission's thoughtful consideration of the existing legal principles underpinning the provision of digital services and products and acknowledging their importance for the economy at large.

The following sections provide ITI's specific comments on different aspects raised in the public consultation. We look forward to continuing to engage on these important and timely topics as the Commission advances the Digital Services Act.

Section I – Safety online

Experiences and data on illegal activities online

ITI membership includes nearly all actors in this complex and multi-faceted space, including Internet Service Providers (ISPs), social media platforms, e-commerce sites, cloud providers, and rightsholders, all of whom are dealing with illegal goods, services, and activities online daily. As the questionnaire seeks very specific examples and input, we share a few examples from our members to illustrate these experiences.

ITI members flag and remove illegal data on a daily basis. Our members have a shared interest in upholding trust in the online ecosystem and are willing to explore policy options best suited to address challenges in particular around illegal content online. Here are some examples:

- During the COVID-19 pandemic, many of our members took swift action to remove illegal content, avoid price gouging of needed goods, and curb the spread of false information about the virus.
- Rightsholders have large in-house teams and employ multiple external agencies to identify and report counterfeit goods being sold via online sales channels. Some of our members indicate that their teams monitor more than 45 online platforms in the EMEA region alone and report hundreds of thousands of counterfeit listings.
- In addition to the removal of listings reported by rights owners, some e-commerce sites also proactively remove potentially problematic listings. These are items flagged by complex rules and models that automatically search for and flag listings that may be counterfeit or infringing in some manner. These sites also continue to develop new technology focused on the proactive detection of infringement. Many e-commerce players have developed sophisticated tools enabling them to profile and detect patterns of fraudulent activity and keep previously suspended users from returning to the site.
- Social media companies employ dedicated teams to monitor content hosted on their sites, in order to ensure timely removal of illegal content.
- E-commerce platforms and classifieds sites have programs in place that help avoid the upload of illegal content and to stop proliferation of dangerous goods.
- Some classifieds sites have also developed sophisticated tools enabling them to profile and detect patterns of fraudulent activity and keep previously suspended users from returning to the site; they also offer consumers protection against the purchase of items that are broken, faulty, or do not match the initial description.
- Smaller companies, which do not have the necessity or resources to employ large teams to monitor content, have partnerships in place to benefit from third-party reporting and automated tools helping them identify and remove certain types of illegal content.

- Enterprise cloud providers require potential partners to undergo thorough Know-Your-Customer (KYC) and due diligence mechanisms in order to gain approval to operate in marketplaces."
- Several companies are working on various initiatives to help better determine authenticity of online content in order to provide greater transparency for consumers. Such initiatives would, for example, allow content creators to include metadata about a piece of content in a secure and tamper-evident way. This would be open, extensible attribution solution that can be implemented across devices, software, publishing and media platforms so that consumers have the ability to decide if the content they are consuming is intentionally fake or misleading.

Measures taken against illegal content

Platforms have an important role to play in removing illegal content online, including proactive measures and **effective notice & takedown (N&T) systems**. Any future initiative on oversight of illegal content should focus on a company's role and its interaction with the content to identify the actors best placed to act. Differentiating where services may have the ability or right (contractual, legal or otherwise) to edit, moderate, or manage content versus where they have technical control but often no access, capability, or the contractual right to alter or remove the data will be important criteria for properly scoping this regulation. A one-size-fits-all approach that would impose the same rules on all digital services would create disproportionate burden for many businesses that do not have the ability to access and moderate content, or do not disseminate content to the public such as cloud services. Such an approach would limit the uptake of cloud technologies across businesses and damage the broader data economy. Additional measures should hence primarily apply to online services that make information available to the public and have the control, technical means, practical ability, and the right to moderate content. For example, an open source B2B cloud platform used to develop blockchain solutions for securing supply chains, or a provider of a private cloud storage service, or analytics tools to help farmers understand crop and weather data, do not have the same business model, nor present the same risk profile when it comes to illegal content, than other consumer-facing services.

Consequently, the DSA should seek to clarify which **sectors or activities require specific transparency criteria, with the objective of strengthening consumer protection standards**. B2B services that are not consumer-facing and are merely providing their business customers with the technical infrastructure or any cloud service that allows its users to host and store private and business content or data should not be subject to such requirements.

Many of our members providing infrastructure services reserve the right to terminate the service provision if terms are violated. For example, if a cloud service provider is made aware of the presence of illegal content or harmful activities on a client website which violates the terms of the cloud services agreements, the cloud service provider can only block access to an entire server, but cannot get access to the individual piece of content to remove it. Instead, they would instruct the customer (or the customer's customer) to remove the notified content. If they fail to do so in a timely manner, the cloud service provider can only suspend access to the server. In short, blocking or removing specific content would in most cases lead to take down of entire services. Software as a Service (SaaS) and Platform as a Service (PaaS) providers face similar challenges. They have the technical ability to take down individual content without shutting down the entire service, however, contracts including data protection provisions and other safeguards often preclude those companies from interfering with the customer's content in any way. In other cases, data stored can be fully encrypted and companies are prohibited by law from monitoring the information and are only able to suspend consumer's access to the entire service. There should be consideration as well of what available and proportionate actions platforms can take where the

customer fails to remove the illegal content, with consideration of what measures may be technically impracticable (e.g. results in indiscriminate or disproportionate removal of legitimate customer content).

While we appreciate it is challenging to **define some types of illegal content at EU level such as those related to freedom of expression at the national level,** given this is the remit of the national legislatures and courts, we think such a definition is highly desirable and important to advance efforts of keeping the Internet a safe place for all. An attempt at achieving a harmonised definition would be to find minimum requirements that are universally agreeable to define illegal content based on solid and confirmed EU case law and national level rulings as per the Commission's proposed approach.

We acknowledge that differing cultural contexts and legal traditions in the Member States regarding freedom of expression may justify the need for specific measures, but we fear that the growing tendency of some EU Member States to "go at it alone" and seek to enforce legislation targeting online content contrary to the **Country-of Origin principle** is worrying as differing national definitions of what is illegal, create a patchy legal framework that creates uncertainty for businesses and undermines the joint goal of all actors involved to reduce illegal content online.

Measures taken against harmful content

The differentiation between illegal and harmful content needs to be maintained. Regulatory efforts should focus on illegal content as defined by existing law – including both civil and criminal infringements, with no distinction being made in the application of the liability rules. **Harmful, but not illegal, content** remains an important topic to deal with and should continue to be addressed separately through appropriate voluntary or co-regulatory approaches, in line with solutions foreseen for instance in the Audiovisual Media Services Directive. For example, we welcome the continued efforts to work jointly with the European Commission and industry players on the EU code of conduct on countering illegal hate speech online. The decision on whether content is harmful and should be removed is greatly influenced by regional or national cultural context. Policymakers should cooperate with companies to develop harmonious solutions vis-a-vis harmful content that fit a certain society through self-regulatory or co-regulatory approaches that promote trust between companies, policymakers and users, and support innovation. We are keen to explore the idea of an **EU-wide project to try and define harmful content online and find regulatory solutions** in conjunction with existing case law and in close cooperation with EU regulators and industry to rapidly address these challenges. In particular, we believe any new regulatory framework should encourage platforms to act diligently and provide for an approach that is proportionate to the potential level of harm.

Measures to protect legal goods and content

Many of our members maintain redress mechanisms for users in instances where content might be erroneously removed, or accounts blocked. This includes counter-notices, which are part of a framework for users to challenge what they believe to erroneous removal of listings. In such cases, escalation teams review decisions on a case-by-case basis. To avoid such situations from regularly occurring, some companies have quality controls in place that take the form of internal audits that review decision making for false positives and false negatives from automations as well as for human error. Where human errors occur, guidance may be rewritten for clarity to reduce recurrence.

Transparency and cooperation

We support the idea of increased transparency and cooperation, and we urge the Commission to consider appropriate and proportionate avenues for achieving this goal. While the Commission reflects on the potential increased costs for public authorities to ensure enforcement and cooperation, it should also

consider costs that all companies in this complex ecosystem currently bear and the desire to balance new reporting obligations with potential burdens on companies throughout the ecosystem. New obligations could lead to **additional costs for companies whilst other alternative approaches to promote transparency might be equally suitable.** For example, many companies already invest in transparency reporting. Any new costs need to be carefully weighed with the benefits that regulatory action could bring for European consumers.

'Notice and action' system for reporting illegal goods or content

There are no harmonised reporting requirements in place for notices filed through platforms which delays notification procedures and adds burden for stakeholders using the processes. In order to foster greater convergence of reporting tools for different types of illegal goods, content, and services, we would welcome a discussion on **basic default criteria and guidelines for 'notice-and-action' systems into an EU-wide harmonised framework, and to create** a number of vehicles including co-regulatory codes of conduct developed jointly by all involved stakeholders and the European Commission. Such codes of conduct would ensure that the best possible technological solutions (e.g. format for submitting complaints), are found for respective industrial sectors in a consultative manner involving all relevant industry stakeholders and can be more easily updated as technology develops. Basic default criteria should include a requirement in the notice to include a hyperlink/URL to the alleged illegal content, a complaint summary, and identification of the person making a complaint.

Content moderation teams

Most of our online platform members already have appropriately trained content moderation teams with the right resources in place. The need for online platforms to install such teams should be based on business model and its likely exposure to illegal content as well as its ability to moderate such content.

Cooperating with national authorities and law enforcement

Our members are committed to working with national authorities and law enforcement to detect and remove illegal content from their sites. However, there needs to be a clear framework that sets boundaries and does not lead to take down of lawful content that could risk impeding freedom of expression and freedom to conduct a business. National authorities need the prioritisation and resources to take action on the information they receive. Today authorities often lack both and bad actors are not pursued to create deterrence.

Trusted flaggers

Trusted flagger schemes can be a useful tool to enhance collaboration among all actors in the timely removal of illegal content online, where a notifier (e.g. corporate entities or neutral third-party organisations) has built a reputation for accuracy and a lack of abuse. Platforms should be encouraged to provide trusted flaggers the ability, through a carefully defined and proportionate process to request a fast-track removal of illegal content or listings for counterfeited goods. While trusted flagger schemes may be an option for illegal content and counterfeit listings, they should not be used for other IP infringements, including for example patent or design infringements.

A cooperative and dynamic trusted flagger scheme should set out the criteria a trusted flagger would need to meet, to obtain, maintain and retain this status. Such systems can bring efficiency gains for both online platforms and rightsholders and create a smoother removal process for illegal content in general.

Know your customer schemes

'Know your customer' (KYC) schemes for commercial users of marketplaces, if developed and implemented in a way that does not introduce disproportionate or burdensome obligations on the parties involved, could create a positive scenario for improving accountability. KYC schemes could for example be helpful to combat fraud and counterfeit products being sold online thereby enhancing consumer protection. Several online marketplaces are already conducting thorough background checks of their sellers as part of their own trust and security processes. Any potential KYC measures should be proportionate, tailored to the variety of business models involved, and developed in collaboration with stakeholders.

The potential introduction of a KYC scheme should consider that the digital services landscape is multifaceted, and a variety of actors would be subject to potential new obligations. There can be challenges in identifying professional users (e.g. limited access to freely available digitized public records at scale), holding up SMEs from accessing services pending clearance. Disproportionate KYC schemes, that could impact the flexible "pay-as-you-go" model on which many cloud-based software or infrastructure services are based, should be avoided if they discourage companies, particularly SMEs, from moving to the cloud.

We recommend addressing any shortcoming through a tailored approach and avoid applying inappropriate constraints on all business-to-business contractual relationship, regardless of the services and the business models. Many of our members already apply due diligence measures to limit illegal activities, including restricting how our services may be used in terms of service. These measures enable them to discontinue the service in case those terms are violated.

We also encourage the introduction of a harmonised definition at EU level of what constitutes a business customer as national definitions are currently diverging or absent in some Member States. In particular, a harmonised list of criteria of what constitutes a business customer would be helpful for companies seeking to comply with potential KYC schemes.

Third-country operators

Ill-intentioned traders selling fake or unsafe products in the EU market put the safety of European citizens at stake and reduce trust in the online economy. Customs authorities are equipped with the power to seize products breaching EU health and safety requirements. However, customs authorities are often unable to verify products due to a heavy workload as well as a lack of resources, training and expertise. For cases involving several customs authorities from different EU Member States, language barriers can further complicate cooperation. Advanced electronic data for postal shipments would enable risk profiling and screening ahead of arrival or even before being cleared for dispatch. Additional investment in enforcement against bad actors when goods are discovered should be a priority.

We encourage the Commission to explore what workable and proportionate measures all actors in the supply chain can take, in conjunction with customs authorities and other government stakeholders, to ensure that products sold online in the EU are genuine and comply with relevant EU rules.

Section II – Liability

We support the roadmap's intention to clarify and upgrade the liability and safety rules for digital services with a view to removing disincentives for voluntary actions to address illegal content, goods or services. There are countless types of digital platforms that offer different sorts of products and services, and the DSA should provide legal certainty in this constantly changing landscape. Clear rules and responsibilities that do not disincentivise companies' actions to limit distribution of illegal content online while being flexible enough to allow for innovative solutions are crucial. At the same time, those players in the ecosystem best suited to take action should do so, while maintaining and clarifying liability exemptions as developed in the E-Commerce Directive.

For example, while intermediary service providers cannot be compelled by a Member State to provide general monitoring of content or activities, this does not imply that service providers cannot initiate certain proactive activities on their own. A number of service providers currently perform voluntary oversight activities to enforce their terms of service and to protect users. Companies need clear rules and responsibilities that do not disincentivise these proactive actions to limit distribution of illegal content online. We welcome the European Commission's acknowledgment that platforms can face a **dilemma when screening content with or without deploying automated tools to screen content** on their sites, as this might remove crucial liability protections. Automated tools for content removal are still in relative infancy and are constantly updated and improved, however, they can still lead to 'false positives' or missed items. Any "voluntary measures" that may be considered under possible options should be very clearly defined as to their scope and limits. For example, the E-Commerce Directive (ECD) does not itself clarify that when an intermediary has voluntarily reviewed content or activities for a specific unlawfulness (or specific violation of community guidelines), it is not deemed to have knowledge of any other ways in which the reviewed content or activities might be unlawful. While there is some guidance on this topic through the Recommendation on tackling illegal content online, ITI recommends providing further clarity.

Section III – Gatekeepers

We appreciate the recognition of the impact assessment that platforms have played an indispensable role in driving innovation and growth in the economy, creating market opportunities and access for businesses of all sizes. In pursuing this initiative, we recognize that the EU must carefully consider how to ensure that it protects important public interests, including consumer welfare, the right to do business, and preservation of competitive markets. Because there has been significant innovation in this space, both in spite of and enabled by large platforms, any *ex ante* regulation should be carefully considered and appropriately targeted.

Definition of gatekeepers

Internet platforms are transversal actors across a global economy and supported by complex supply chains. As the internet allows consumers to increasingly benefit from fully integrated products and services, it also creates diverse types of relationships between different suppliers. As the Commission considers these relationships and market characteristics, we urge recognition of the flexibility that has enabled the internet economy to flourish and allow citizens, businesses, governments, and consumers to connect with each other and others in remarkable ways.

The scope of this effort will be extremely important, as which companies may be considered gatekeepers and therefore subject to potential additional regulations will have significant impact on the ecosystem.

The nature of a platform and its size should not automatically be perceived as harmful, particularly given the demonstrated benefits the platform economy brings to all users, including to deliver trust, reach and efficiencies. We therefore encourage the Commission to consider focusing the scope and test for intervention on actions and conduct, rather than companies. The characteristics of a market, specific activities by a platform, and interactions with other platforms and with users will be more indicative of a potential market failure than just the characteristics of a particular platform, such as market share, number of users, or number of services offered.

Similarly, it is important to consider how gatekeeper definitions may apply to companies with multiple verticals. Due consideration is needed in these cases. The roadmap should focus on specific conduct and actions, rather than the size of one or more business units. Furthermore, the variegated nature of online platforms and the incentives driving specific decisions by platforms must be taken into account when assessing conduct. An incentive to protect the user against illegal and harmful content, fraud, data violations or security threats might be to the immediate detriment of specific business users for example when a product or service is delisted. This is however often needed in order to sustain consumer trust to the benefit of all users.

Emerging issues

The Commission's thinking outlined in the previous roadmap document referred to certain platforms having become or acting as "gatekeepers" but does not actually clarify what that entails and the potential consumer harm, anticompetitive effects on the market. **One should not single out certain companies based exclusively on their size (*market share, number of users, amount of services…*) or impact**.

In its previous IIA, the Commission notes the important role of network effects, which is an essential factor in the online ecosystem. Network effects bring additional benefits to users with each additional user that participates in a platform, but it does not necessarily eliminate competitors or stifle innovation. However, we understand there can be concerns around network effects, potentially resulting in user lock-in or limiting new entrants on the market. In this context, better understanding how certain practices may impact a specific market and correcting potential imbalances and failures may be useful, as long as such tools and rules are carefully assessed in order not to negatively impact consumer choice, innovation, and rapidly evolving markets and business models.

Regulatory options

As identified in the impact assessment, this consultation sits at the intersection of several initiatives that are already in place or also in consultation, such as P2B, the new competition tool, and various consumer protection and data privacy laws. Due consideration should be given to this consultation as to whether these themes are already adequately captured by those efforts, so as to avoid duplication, confusion, or negative impacts on the marketplace.

It will be important for the Commission to give the still new P2B regulation time to come into effect and be evaluated for where it is or is not successful, and what, if any, alterations may be necessary to strengthen or improve it. Adding new requirements, or building upon those already in the P2B regulation, without first assessing how they are working, could create additional challenges, costs, and harms to both platforms and consumers. Any new initiative should align with existing rules, especially those in the P2B regulation.

Similarly, we urge the Commission to consider how this potential regulation will co-exist with its other digital policy goals. Firstly, given the multi-sided nature of platforms, regulatory intervention on one side

should not undermine benefits on the other. As outlined above, a platforms' efforts to act responsibly in protecting consumers, one of the goals of the Digital Services Act, may be perceived as detrimental to its business users. Secondly, these regulatory efforts many overlap with the New Competition Tool, given its similar policy goals. This may lead to similar or duplicative burdens for companies. Legal certainty is critical for companies of all sizes, and the Commission should ensure that companies, including gatekeepers, have a clear legal environment in which to operate.

The impact assessment noted a number of potential practices that could be reviewed, limited, or prohibited, as well as new transparency requirements that may be added to gatekeeper platforms. We recognize the challenge in creating *ex ante* restrictions or limitations, as the Commission does not want to create unintended consequences that could needlessly hamper innovation, consumer experiences, or business growth. We urge the Commission to carefully consider the impact of potential limitations, in order to prevent any regulatory failure from overbroad instruments or poorly tailored requirements. Any potential limitation to behavior or business practices should be narrowly focused to achieve the intended goal. Similarly, the Commission's proposal should reflect the importance of proportionality for a regulation based on the action or conduct deemed inappropriate. Similarly, ex ante regulations, such as a 'blacklist' of prohibited practices, would require very careful consideration in relation to a dynamic industry that has multiple business models, types of users, types of business partners, and existing tools in place to address the issues at stake. Any new regulation should take into account how business users interact with and benefit from greater transparency and communication with online intermediation services.

Section IV – Other issues

Online advertisement

We acknowledge the European Commission's interest in better understanding how online advertisement is impacting European consumers. It is important to note that the online advertising ecosystem encompasses a large range of actors including whole industries, third party advertising agencies and publishers who all rely heavily on revenues generated via the online advertising business. We therefore suggest separating the discussions on online advertising and the DSA, as online advertising issues fall outside of the scope of an effort aimed at content oversight and intermediary liability and risk impacting a broad range of industries that are currently grappling with the economic impact of the COVID-19 crisis and increasingly relying on digital platforms as vehicles to reach customers.

Smart contracts

Smart contracts are lines of code to facilitate the execution of specific elements of a transaction. They are not using artificial intelligence nor analytics software; neither do these replace "traditional" contracts (i.e. agreements written in plain terms). Therefore, we do not currently perceive any difficulty, nor see a need for a regulatory framework related to smart contracts (neither, for instance, to (i) strengthen their enforceability; nor to (ii) contain mechanisms to halt their execution). The rationale is that the contract documents (traditional contracts), use plain words and can and should therefore properly and sufficiently include such mechanisms. These traditional contracts also guarantee the enforceability of the contract that describes the project or commercial transaction which involves the use of blockchain technology (and hence the lines of codes used to support the execution of this commercial transaction). These lines of codes (called "smart contracts") should not replace traditional contracts entirely in the short term, they should rather support the automated performance/execution of certain elements of the transaction described in such traditional contracts.

Section V – Governance

Governance and enforcement

Given the ongoing legislative initiatives launched by a number of Member States, there is value in exploring a **single EU-wide coordinated oversight model**, be it a body or a process within the current institutional setting, that would enhance legal certainty by providing guidance to consumers and companies, and help the latter take reasonable, feasible, and proportionate measures. The oversight mechanism should not interfere with responsibilities within the jurisdiction of the Courts. This model should provide predictability, be co-regulatory in nature, provide a consultative role for industry and civil society, be based on clear rules and procedures as well as an open and transparent decision-making process. Any oversight model should fully respect the Country-of-Origin principle. There are existing examples of cooperation between national regulators in the absence of an EU agency that have proven successful, including the EU's telecoms regulator BEREC and similar groups in the pharma or energy sectors.

We support the goals of increasing legal certainty, clarifying roles, and defining responsibilities for actors in the online context, i.e. by reviewing and bringing more clarity to the framework. We are committed to working with the European Institutions to forge a balanced framework preserving the current limited intermediaries' liability rules and rights of third parties, for a healthy online ecosystem. We support the European Commission's thoughtful consideration of the existing legal principles underpinning digital services and products and acknowledging their importance for the economy at large. We welcome plans to gather robust stakeholder input and develop well-tailored solutions for specific, well-defined challenges. As sanctions or other enforcement mechanisms are considered, the Commission should strive to carefully define the concept of "systemic failure" and take into account several aspects such as the nature of the infringement, gravity, intent, attempts to mitigate and precautionary measures among other factors.

We believe that while there might be scope to improve the regulatory framework in a targeted fashion, existing legislation should be transposed and enforced first, before introducing new obligations for digital services. This includes the Recommendation on measures to effectively tackle illegal content online, the Copyright Directive and the Audiovisual Media Services Directive, as well as the Platform-to-Business (P2B) Regulation. For example, the 2019 P2B Regulation already introduced comprehensive reporting obligations for platforms. Instead of introducing new requirements, we urge policymakers to assess the workings of the P2B obligations at the occasion of the law's first review in 2022.

We also believe that boosting **enforcement capabilities**, especially in the Member States and for relevant authorities, is a crucial step towards reducing proliferation of counterfeit goods. Currently, there are hundreds of customs authorities and domestic law enforcement agencies across Europe that do not successfully cooperate, in many instances due to a lack of personnel and resources more broadly, as well as due to language barriers. A refocusing of priorities for enforcers and an increase in resources to enable them to act effectively against counterfeiting, including through the power of issuing meaningful sanctions should be a central part of a renewed agenda on this topic. Further, cooperation between all stakeholders in the process needs to be advanced, in particular between digital service providers, authorities and IP rights holders.

When considering the need for an **updated governance framework** to support digital services regulation, the **following principles** should be considered:

- An updated framework should strive for maximum harmonisation and coordinated oversight to prevent fragmentation of the Digital Single Market (DSM).
- Regulators in the digital services space should cooperate closely with other relevant regulators (privacy, competition, consumer, audiovisual, cybersecurity, etc.).
- An updated framework should be based on clear and transparent procedures, to ensure regulatory certainty and accountability. Company specific remedies and decisions should be regularly reviewed and should be taken in close cooperation with industry.
- An updated framework should include appropriate procedural safeguards such as right to good administration, rights of defense, ability to review the regulator's decisions, right to a fair hearing and ability to contest decisions.

* * *