DIGITALEUROPE

8 SEPTEMBER 2020

Digital Services Act consultation response

Executive Summary

DIGITALEUROPE's membership fully supports the European Commission's ambition to strengthen the digital services market in the EU. We agree that clarity is needed on the role and responsibilities of online platforms to make the internet safe.

Illegal and harmful content is too prevalent on the internet. Our members do not seek additional liability exemptions, but rather want a legal framework that allows them to tackle the problem and play their part in creating a healthier online environment. This will help to increase the levels of trust that European citizens have in digital services.

Online intermediaries, rights holders, users, government and law enforcement all have a role to improve the safety and trust in the Internet economy.

The Digital Services Act should complement and provide greater clarity to the fundamental principles of the E-Commerce Directive (ECD):

- It should make clear the roles and responsibilities of different actors online, and incentivise rather than discourage intermediaries to remove illegal and harmful content.
- Given its wide-ranging importance to the functioning of the internet (and the potential for unintended consequences), it should retain the simplicity of the ECD and be narrow in its focus.
- Where needed, it should be accompanied by additional issue-driven (voluntary or regulatory) measures to tackle specific problems, as has been the case in areas such as product safety, counterfeits, hate speech, terrorist content, copyright infringement, and disinformation.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Table of Contents

Part I. How to effectively keep users safe online

Illegal goods on online platforms

Illegal goods are too prevalent in society and on the Internet and of particular concern for DIGITALEUROPE's members is the proliferation of counterfeits online. As businesses and customers have moved online, so have counterfeiters. Online sales and distribution of counterfeits occur through web stores, marketplaces and elsewhere, just as offline distribution uses multiple channels, including physical marketplaces.

IPR infringements cause significant societal and economic harm, disrupt fair competition, and create reputational damage to brand owners. Counterfeited goods may also pose potential health and safety risks to European consumers in addition to creating security vulnerabilities within internet networks.

DIGITALEUROPE submitted a response to the recent EU Counterfeits and Piracy Watchlist organised by DG Trade where it provided evidence of troublesome online and offline marketplaces.

Illegal goods from third countries

DIGITALEUROPE members have experienced sellers based in third countries selling dubious products in the EU market, that are counterfeit or breach EU health and safety requirements. This is problematic as such products put the safety of European citizens at risk and more generally reduce consumers' confidence in the online economy. Rightsholders rely on notice and takedown procedures as a critical aspect in their fight against counterfeit products.

Impact of COVID-19

It's hard to tell whether illegal goods were more easily accessible as we are not aware of a study undertaken to compare results pre and during the pandemic, not just online but also offline. Anecdotally, at the start of the outbreak, some members flagged trends in specific product types such as masks, supplements claiming to prevent or cure COVID-19, medical equipment and personal protective equipment. Such patterns are now declining.

Some of DIGITALEUROPE's members worked with DG Justice, Europol, national enforcement bodies and brands like 3M to address attempts at price gouging, misdescription or use of brands for counterfeiting. These members have been regularly engaging with EU and national authorities to provide updates on the effectiveness of systems and programs, as well as highlighting trends. Their submissions can be found on the DG Justice website.

Experiences with reporting illegal goods

DIGITALEUROPE has a diverse membership, which includes both online platforms and companies whose products often appear as counterfeits or parallel imports in online platforms. Many DIGITALEUROPE members report links promoting counterfeit goods through multiple platforms in the EU.

Many platforms provide rights holders with a system which allows them to search, report and track whether a notice was accepted and content was removed. DIGITALEUROPE members report varying experiences, particularly when reporting counterfeit goods. Some well known platforms take action to remove illicit or illegal listings once notified, however the speed at which listings are removed varies. Members also report difficulties with the reappearance of copies of previously notified content.

Costs

For years, DIGITALEUROPE members have actively supported efforts to reduce the amount of illegal content online. This has involved heavy investment in technologies, processes and people, and close and ongoing work with regulators and competitors to protect internet users. Considerable costs are incurred by both platforms, who have implemented technological and human content moderation teams, and manufacturers who have sophisticated in-house brand protection teams who identify and report counterfeit listings. These costs are especially burdensome for SMEs.

Measures to address illegal content

Illegal vs harmful

The DSA should clearly distinguish between illegal, and lawful but potentially harmful content. Harmful content is contextual, difficult to define, may be culturally subjective and often legally ambiguous. Harmful content should therefore not form part of the liability regime. Where Member States believe a category of content is sufficiently harmful, the government should make the content illegal or engage in issue-specific measures to tackle harm. We refer to the recent decision of the French Constitutional Council in which ruled that the proposed 'Avia law' to regulate online hate speech was unconstitutional and infringes freedom of expression and communication.

At the same time, it is desirable for society that intermediaries have the capacity to moderate lawful but potentially harmful content. Not all content is suitable for all platforms and the communities they serve. The DSA should clarify that it is within the discretion of the service provider to decide which content is sufficiently harmful to warrant removal. The DSA should incentivise rather than discourage intermediaries from removing illegal and harmful content.

Addressing illegal content should be done in a meaningful, well-targeted and proportionate way. However, not all companies have the necessary technical means, practical ability, or the right to moderate illegal content. Digital services are a very heterogeneous group and it is important the DSA takes this diversity into consideration. Cross-industry cooperation and partnership with civil society organisations can bring positive results in tackling illegal content online. The EU Code of Conduct on countering illegal hate speech online is a good example thereof.

Timeframes for removal

Online intermediaries should remove illegal content without undue delay once they have actual knowledge of illegal activity. In addition, given that the fast removal of illegal material is often essential in order to limit wider dissemination, online intermediaries should have a clear policy available for handling notices, including an indicative timeframe for review, so that notifiers have confidence that notices will be considered and acted upon swiftly. Such notification systems should be accessible to all actors and easy to use.

Specific timeframes for the removal of content should not be mandated in law as intermediaries should not be forced to prioritise speed of removal over careful decision-making. Very short deadlines may incentivise illegitimate takedowns of

lawful content and pose a serious threat to freedom of expression and information. The decision of the French Constitutional Council striking down the proposed 'Avia Law' underlined that the one hour deadline does not allow affected parties to obtain a decision from the judge before the content is made inaccessible.

Notice & action

DIGITALEUROPE supports maintaining a notice and takedown regime. However, the current system for sending and receiving notices is not formalised. It lacks clarity and consistency, which leads to longer handing times than necessary in some instances. In order to facilitate the expeditious removal of illegal content, a notification should contain all the necessary information for the recipient to act without communicating further with the sender. It may be desirable to establish (and harmonise) the minimum information needed for a notice to be actionable (such as unique URL,video timestamp, the alleged infringement type or illegality, status of notifier) however, such criteria should be technology-neutral to accommodate the diversity of digital services.

Equally, given that the fast removal of illegal material is often essential in order to limit wider dissemination, the receiver of the notice should have a clear policy available for handling notices, including an indicative timeframe for review, so that notifiers have confidence that notices will be considered and acted upon swiftly. Such notification systems should be accessible to all actors and easy to use.

Any formalisation of the notice and action system should not capture services enabling private communication between a finite group of users, in accordance with the definitions provided in the European Electronic Communications Code.

Counter-notices

DIGITALEUROPE members maintain easy-to-use webforms to simplify the process of requests to reconsider and reinstate content (or user accounts) that users feel were removed or closed in error. Our members take their responsibilities seriously in removing and addressing violations of terms of use but recognise that they are not perfect, and these forms improve their ability to review and correct possible errors. Once received, they review the complaints received to ensure that the procedures were followed accurately. Items are reinstated if there was an error and remain off the service if not.

Trusted flaggers

The use of trusted flaggers systems, where specialised entities with specific expertise (e.g. sophisticated corporate entities in the case of goods or neutral third party organisations in the case of content) in identifying illegal content or goods have access to dedicated structures for detecting and identifying such content online, could be encouraged. The use of sophisticated trusted flaggers schemes can have a twofold advantage: 1) for trusted flaggers: the infringing listings could be taken down more swiftly; 2) for platforms: there would be higher confidence in the accuracy of claims. An effective system will have a balanced and shared responsibility of all

players in the value chain, with the participation of government agencies, police and law enforcement, civil society and rightsholders.

The use and role of trusted flaggers systems should be tailored to the type of content in question and the specialisation of the trusted flagger as well as the business model of the provider. Online intermediaries should be free to choose their own trusted flaggers, determine the specific privileges and be able to act on their own judgment, however, they must also provide transparency in terms of how entities or organisations qualify as a trusted flagger and how they determine their specific privileges.

Trusted flaggers should not be excluded from good faith requirements or from associated sanctions for those who are proven to persistently abuse procedures by sending claims which have no legal basis. If there are too many complaints from third parties about a trusted flagger and its notifications and it is clear that a trusted flagger is either reckless in its reports, negligent or error-prone, then the trusted flagger status would be withdrawn and the entity would need to revert to reporting via a standard notice and takedown procedure.

KY(B)C

Some stakeholders have also proposed introducing ‘know your business customer’ obligations to the Digital Services Act. Several DIGITALEUROPE members already conduct background checks on business users voluntarily. Basic verification of business identities can be useful to reduce the prevalence of counterfeits and other fraudulent activities, disincentivise bad actors online and aid law enforcement.

The introduction of a KY(B)C scheme should consider the diversity of digital services and the variety of actors who would be subject to potential new obligations. Obligations should be proportionate and include appropriate safeguards to protect the privacy of users in the course of legitimate and lawful activities. Requirements should be tailored to the variety of business models involved and developed in collaboration with stakeholders.

A harmonised definition at EU level of what constitutes a business customer would be useful as national definitions are currently diverging or absent in some Member States.

Sanctions for repeat offenders

All notifications should be made in good faith. Those who are proven to persistently abuse “notice and takedown” procedures by sending claims which have no legal basis should be held accountable and intermediaries should be permitted to ignore their notices on the grounds that such notices do not convey “actual knowledge”.

Freedom to provide lawful services

Intermediary service providers should be free to provide any lawful service they develop. These services should not be subject to any a priori licensing regimes or approval schemes for launching or changing certain types of legitimate services.

There should be no prohibition on offering legitimate services where it is not technically possible or commercially feasible to apply content regulation obligations or lawful intercept obligations. Any obligation for an intermediary service provider towards such a legitimate service should be limited by the concept of feasibility.

Best practise forums

DIGITALEUROPE in addition encourages forums for cooperation such as EU product safety pledge, Memorandum of Understanding on Counterfeiting, and the EU Code of Conduct on Disinformation. Participation in these forums should not, however, be obligated. For example, engagement in such forums would pose a disproportionate burden for SMEs.

Informing consumers

Some e-commerce platforms already voluntarily notify customers of unsafe products sold by third party sellers based on information from manufacturers, market surveillance authorities or public recall websites. While such practices do not necessarily work in all circumstances and across all platforms, they could be seen as a way forward with respect to the online sale of unsafe illicit products.

Actions to address online scams and other unfair practices

Members invest millions of euros to ensure safe and appropriate experiences on their services. Machine learning is used - in combination with dedicated user safety experts and other manual detection, review and enforcement methods - in some cases to look for transaction patterns or other behaviours that reflect suspicious account behaviours indicating a potentially hijacked or abused account. However, as noted above, there are limits to machine learning, as well as the ability of humans to make judgements on less obvious or more complex issues raised in notices or identified through machines.

Many services review business users before allowing them to trade, and block attempts to register fraudulent accounts using stolen credentials. DIGTALEUROPE's members use a wide variety of tools that are designed to comply with European rules on unfair practices.

Child protection

It is essential to enact and enforce laws against the possession, production, and distribution of child sexual exploitative imagery worldwide, and to both build and fund the necessary infrastructure to ensure safe rescue, support and recovery for victims of child sexual exploitation.

Grooming, the process by which predators manipulate children for sexual exploitation, recruiting to terrorist organisations or other purposes, is facilitated online when predators use the internet to make contact and develop relationships with children and young people.

The industry's approach to combating child predation includes creating innovative technology tools; providing education and guidance; establishing robust internal policies and practices for moderating content and addressing online abuses; and collaborating with government, industry, law enforcement, and others. A good example of this is the Project Protect of the Technology Coalition.

Issues with operating systems to address illegal content

Different systems for different services encounter different issues. For example, some members experience variations in speed and how listings are taken down. Automated responses that fail to understand the specific legal concerns raised. As noted above, there are limits to machine learning, as well as the ability of humans to make judgements on less obvious or more complex issues raised in notices or identified through machines.

Legal fragmentation and definitional vagueness

Some Member States have begun to consider or to impose country-specific content moderation requirements on online intermediaries. As the Member States move to increase these obligations, providers face a growing compliance challenge, one that could become unworkable and threaten the integrity of the Single Market. Any new EU-level rules in this area should promote the maximum degree of harmonisation possible, to ensure that providers are able to comply with a single set of rules across all EU markets.

Jurisdictional differences in the definitions of illegal content impose significant challenges to effective content moderation. Vagueness in definitions of certain content, such as hate speech, place a burden on technology companies to attempt to ascertain the intent of the speaker often with little to no context. Language changes rapidly. Also, slang, abbreviations, symbols, and other imagery can have many legitimate uses absent context or clarity of intention – neither of which may be available to or understood by artificial intelligence or human moderators. Yet, when the penalties for failure to remove the illegal hate speech are significant, technology companies will be forced to err on the side of blocking lawful content. This chilling effect on speech is a major criticism of the NetzDG law in Germany.

Jurisdictional conflicts

When content is made available globally, as is the case in many digital services, managing varying content laws by jurisdiction imposes onerous geo-blocking burdens or forces services to apply the most restrictive content policies worldwide. The net effect is a jurisdictional conflict resolved only by overinclusive restriction of speech, or by limiting access to services by geography. Either case undermines free and fair access to the open internet.

Privacy conflicts

A key challenge in this context is Europe's ePrivacy regime. When scanning for illegal content online, particularly child sexual abuse imagery (CSAI), internet service providers need to balance users' privacy rights with child safety and law enforcement/government requests, particularly in geographies with strict privacy and communications secrecy laws where a breach may result in financial penalties or criminal charges.

It is critical to ensure that when evaluating, for example, any formalisation of notice and action systems, or matters of cooperation with law enforcement authorities, that the obvious tensions with human rights, such as the protection of privacy and personal data (such as laid down in Europe's Data Protection Laws) are carefully considered to ensure that an appropriate balance is maintained, and that any resulting legislation is particularly clear in this regard and appropriate redress opportunities and independent and effective oversight are in place.

Harmful content

As a principle, it is both legitimate and desirable that platforms restrict types of lawful content they do not consider, for whatever reason, appropriate for the service they provide. It is desirable for society that online intermediaries have the capacity to moderate lawful but potentially harmful content. Not all content is suitable for all platforms and the communities they serve. The Digital Services Act should clarify that it is within the discretion of the service provider to decide which content is sufficiently harmful to warrant removal.

Detecting and reporting suspicious behaviour

Some stakeholders perform certain voluntary activities at the moment in order to enforce their terms of service or to protect users, among which to detect certain suspicious behavior. However, suspicious behaviour is contextual, difficult to define, may be culturally subjective and often legally ambiguous. The Digital Services Act should therefore clearly distinguish between illegal, and lawful but potentially harmful content, like for instance suspicious behavior of some sort. DIGITALEUROPE is of the opinion that service providers should not be obligated to detect and report suspicious behaviour. One of the key cornerstones of the ECD is the ban of a general monitoring obligation. Suspicious behaviour should not form part of the liability regime. The Digital Services Act should clarify that it is within the discretion of the service provider to decide which (flagged) content is sufficiently suspicious to warrant reporting to the relevant authorities.

Transparency on content removal

Improving transparency online will increase users' trust in the Internet and help foster Europe's vision for 'human-centric' digital services. In all cases, it is important to consider the desired outcome from such transparency and intended audience (law enforcement, users, etc.) to ensure proportionality.

For example, in the case of content moderation, intermediaries should be clear about when and why they take down content. Users have a right to know when intermediaries remove content because it is illegal, otherwise harmful or breaches T&Cs; such transparency is an essential component of platforms' accountability to their users. At the same time, different types of content may merit different levels of transparency—for instance, providing notice to users might be appropriate in cases of suspected copyright violations, but inappropriate in cases of child sexual abuse imagery where there may be ongoing law enforcement investigations. Given that many leading online service providers already publish periodic transparency reports, these should be leveraged to the maximum extent possible.

Transparency of algorithmic recommenders

Whilst DIGITALEUROPE supports the need for transparency, it cautions against algorithmic transparency requirements which could risk disclosing trade secrets or allow bad actors to 'game the system'. Any transparency obligation should comprise protective measures against passing on business secrets. Under no circumstances should consideration be given to general provisions which make disclosure of concrete algorithms obligatory, since in many cases they constitute a core element of a provider's business model. The revelation of too much information about the functioning of algorithms can also lead to them being compromised by fraudulent players (hackers, spammers, etc.), which can ultimately harm the consumer. Rather, the publication of generic and general information should be required at most. The recently revised Consumer Rights Directive and the Platform to Business Regulation have already introduced proportionate obligations for online marketplaces in this regard.

On many online services, users already receive information on why certain content or products are recommended to them such as "other people that bought X also bought Y", "inspired by your browsing history" or "based on what other consumers with similar interests". In addition, with Directive 2019/216 Enforcement and Modernisation coming into force, online marketplaces will have to provide the main determining factors for rankings. This provision reflects a careful balance between the consumers' interest in transparency and operators' interest in safeguarding proprietary technology, business secrets and protection against manipulation attempts by rogue players.

Transparency reports

Transparency reports should be strongly encouraged. However, they should be proportionate for all players and not pose an undue burden for SMEs. To ease reporting, it might be desirable for the EU institutions to develop a best practice for transparency reports. In developing best practice, it is important that the transparency report exclude unnecessary or confidential information, including information that would be counterproductive or could be used to circumvent measures.

Erroneous removals

Erroneous removals can be limited by harmonising and formalising the current notice and takedown regime. To this end, a notification should at least contain all the necessary information for the recipient to act without communicating further with the sender. It might be desirable to establish the minimum information needed for a notice to be actionable (such as unique URL, video timestamp, the alleged infringement type or illegality, status of notifier) however, such criteria should be technology-neutral to accommodate the diversity of digital services.

To limit erroneous removals it is also important to clearly distinguish between illegal, and lawful but potentially harmful content. Harmful content is contextual, difficult to define, may be culturally subjective and often legally ambiguous and therefore more prone to erroneous removal, which affects fundamental rights such as freedom of speech. Harmful content should therefore not form part of the liability regime.

To limit erroneous removals all notifications should be made in good faith. Those who are proven to persistently abuse “notice and takedown” procedures by sending claims which have no legal basis should be held accountable and intermediaries should be permitted to ignore their notices on the grounds that such notices do not convey “actual knowledge”.

Reappearance of illegal content

Some members have noted problems with reappearances of illegal content, goods or services. Reappearances of illegal content, goods or services, in general, is the result of continued attempts at abuse. Eliminating all abuses all time is as tricky online as offline. There are many factors outside the control of a platform that they cannot control. For example, millions of genuine identities have been stolen through cyber-crime and are available to register new accounts. The variety of illegality means different illegal content may be posted even when previous content is removed. Similar content can occur for many reasons that are not always apparent to humans. Some content is not recognisably identical to a machine, some goods are not clearly the same when information about them appears, etc.

Where a user is found to repeatedly post illegal content or violate T&Cs on a platform, despite a number of takedowns, platforms may suspend the account on a temporary or permanent basis. If an account is suspended or closed, the platform should make clear to the user the reasons for the action when it is appropriate to do so. In addition, platforms should have a transparent policy available for when and how an account will be suspended or frozen.

Some stakeholders have discussed the use of automated tools to scan for the reappearance of illegal content. DIGITALEUROPE is strongly opposed to the mandated use of automated scanning tools. For many services, it may not be proportionate to deploy automated scanning given the relatively small number of occurrences, the inaccuracy of automated tools and the ability of bad actors to evade them.

Use of automated tools for content moderation

DIGITALEUROPE firmly believes that the use of technological solutions for online content moderation should not be mandated by law. Content moderation technologies are being used increasingly by a broad range of internet companies. While breakthroughs in machine learning and other technology are impressive, the technology is far from perfect. Misclassification of content remains a challenge, and machine learning tools are vulnerable to adversarial examples, even based on tiny changes to images that are imperceptible to the human eye. Besides, such technology is unable to discern differences in context and meaning that can be critical to determining whether content is legal or not. With regard to products, if a trader uses a gallery image of a genuine product, it is difficult to determine if a product is illicit or counterfeited from the ad/link itself. It is therefore difficult to see how an automated tool could determine if a product, the subject of the listing, is genuine or fake.

Policymakers must understand these limitations and should not mandate the use of automated content analysis tools or impose time limits on responding to notifications of illegal content, which in practice will necessitate the use of automated filters to comply with the law. The DSM Copyright Directive has already imposed a de facto requirement to use filtering technology. This approach should not be followed in future legislation.

Responsibilities for intermediaries deeper in the internet stack

It may be technically difficult for digital services deeper in the internet stack to identify or locate users of the services principally involved in illegal activity, without notification. For example, currently it is technically impracticable for cloud infrastructure service providers to remove or disable specific pieces of customer content. Any obligation to remove or disable access to illegal content should be first on the customer who has made available online the content. Services deeper in the internet stack acting as online intermediaries should be required to take proportionate actions where the customer fails to remove the illegal content, unless technically impracticable (e.g. results in indiscriminate or disproportionate removal of legitimate customer content).

Responsibilities of other stakeholders

Increasing the funding and capabilities of Member State enforcement authorities is one crucial way to help stop the proliferation of unsafe and counterfeit goods from entering the EU market. Customs and market surveillance authorities lack the resources to tackle bad actors in both the offline and online world. We, therefore, urge the Commission to raise awareness and enforcement of product safety and IPR infringements within Europe. Intergovernmental cooperation to act against sellers outside the EU can also be helpful.

In order to facilitate expeditious removal, when authorities discover unsafe or counterfeit products, they must provide clear, structured, actionable information to

online services. This includes minimum data requirements for RAPEX notices in SafetyGate or specific tracking numbers from seized packages.

Further, cooperation between all stakeholders in the process needs to be advanced, in particular between digital service providers, authorities and IP rights holders. Voluntary initiatives such as the provision of digital exemplars to collective projects that provide accurate “fingerprinting” in order to facilitate analyses of flagged illegal content should be encouraged.

Sanctions

Any sanctions should be based on systematic violations, where there has been a sustained failure to comply with obligations, rather than one-off events or individual pieces of content. The DSA should make clear what constitutes systematic violations.

Sanctions and fines should be proportionate to the service itself, rather than the overall corporate ownership. Any fines should be based on a sliding scale – in other words, a lower percentage for first infractions that increases with each subsequent violation. They should not be likely to lead to the restriction of lawful content, nor impinge fundamental rights such as the right to freedom of expression.

Part II. Reviewing the liability regime of digital services acting as intermediaries

Definitions in the E-Commerce Directive

The internet landscape has changed significantly since the adoption of the E-Commerce Directive (ECD), but DIGITALEUROPE strongly believes that these three specific categories of services (‘mere conduits’, ‘caching services’ & ‘hosting services’) remain sufficiently clear and complete for characterising and regulating today’s digital intermediary services.

This categorisation is clearly understood and defined in relevant case law and therefore we would not wish to see a change to it.

Knowledge standard

As regards the hosting services’ liability exemption for third-party content or activities, DIGITALEUROPE believes the knowledge standard has been essential to the development of an innovative internet economy in Europe and the protection of fundamental freedoms such as freedom of expression and respect of user privacy. The rule that hosting services cannot be held liable for their user’s wrongdoings as long as they act expeditiously when they have actual knowledge of specific infringements achieves the right balance of protecting those rights whilst allowing timely, proportionate actions against illegal content and activities. A stricter liability regime holding platforms liable for content they are not aware of, or predicating

liability exemptions on proactive measures, would have prevented a whole range of innovative services from entering the market and resulted in removal of lawful content. Given its importance for the functioning of the internet, the liability exemption provided in the ECD should be maintained in the Digital Services Act, upholding the principle that individual users are ultimately responsible under the law for their online behaviour and the content they post.

Control standard

The ECD's safe harbours for 'mere conduits', 'caching services', and 'hosting services' imply that these intermediary service providers have neither knowledge of nor control over the information which is transmitted through or stored on their service. DIGITALEUROPE strongly believes that the knowledge and control standards remain as relevant today as they were twenty years ago and should continue to be interpreted in light of EU acquis and jurisprudence.

DIGITALEUROPE acknowledges that today's online ecosystem encompasses a wide range of digital intermediary services, in particular in the hosting services category where varying levels of content intermediation, functionalities and accompanying risk profiles warrant heterogeneous responses to tackling illegal content. These responses should precisely be defined in terms of service-specific responsibilities and pragmatic remedies, not through changing interpretations of liability rules and concepts such as 'actual knowledge' and 'editorial control'. The contrary would inevitably result in legal uncertainty and barriers for countless types of digital services, affecting their ability to innovate and scale.

Voluntary measures clause

A number of service providers currently engage in voluntary measures to better enforce their terms of service and to protect users. Intermediary service providers are concerned that such voluntary monitoring carries a risk of depriving the service provider of the safe harbour protection provided by the ECD. For example, the ECD regime does not contain a provision which ensures that, where an intermediary service provider has voluntarily reviewed content or activities for a certain type of specific unlawfulness (or for a certain type of specific violation of its community guidelines), the service provider is not deemed to have knowledge of any other ways in which the reviewed content or activities might be unlawful. DIGITALEUROPE believes a provision providing this clarity would be welcome. This would also enable smaller platforms and startups to develop practical solutions that suit their scale.

Ban on general monitoring

Any obligation to introduce general monitoring would pose significant risks for freedom of expression and fundamental rights. A general monitoring obligation would also have a negative effect on competition and the market entrance of new actors. DIGITALEUROPE members strongly support that this principle is maintained in the upcoming review of the liability regime.

While intermediary service providers should not be compelled by a Member State to provide general monitoring of content or activities, this should not prevent online intermediaries from taking voluntary steps to try to reduce the prevalence of illegal and harmful content on their platforms. We welcome the European Commission's acknowledgment that platforms can face a dilemma when screening content, as taking these voluntary and responsible steps could expose online intermediaries to increased concerns around liability. We would welcome that the European Commission's legislative approach considers options on how to alleviate this situation but any voluntary measures clause that may be considered under possible options should be very clearly defined as to its scope and limits.

Part III: What issues derive from the gatekeeper power of digital platforms?

Digitisation is pervasive – it touches every industry – and any new regulatory instrument or tool should apply to the economy at large. There is no sound basis for singling out particular sectors or types of "platforms." In the consultation, the term "large online platforms acting as gatekeepers" is used to describe what is a very broad and heterogeneous collection of companies that engage in online activity. EU competition law is in place to address any conduct engaged in by market operators, including online services that may interfere with the proper functioning of a market. Other regulatory mechanisms are available to deal more specifically with other policy issues, such as consumer protection or data protection rules. DIGITALEUROPE understands that the Commission is concerned about the duration of antitrust investigations and its ability to intervene before irremediable damage to markets has been done. However, the Commission already has effective tools to expedite its investigations such as the recent use of interim measures in the Broadcom investigation.

Furthermore, any initiatives should first await the impact of recently adopted P2B Regulation. This Regulation sets new requirements for all online platforms no matter their size or market power, precisely recognising that a natural differential in negotiation powers between platforms and business users bears risks. However, it explicitly limited intervention to targeted measures proportionate to the evidence of market failure, which remains limited.

An aspect not reflected in the consultation questionnaire is that of judicial safeguards, procedural fairness and respect for rights of defence for companies in the scope of a potential gatekeepers regulation. Speed of enforcement should not come at the cost of due process. Where the intervention is significant, as is the case with measures currently discussed, companies should have the possibility to appeal remedies with authorities and ultimately courts. Especially outright prohibitions of business practices have a significant risk of regulatory failure and require careful assessment of the effects on competition, innovation and consumer welfare.

Criteria to define 'gatekeeper platforms'

Ultimately, what determines a company's ability to employ practices raised as concerns in this debate is its market power that forms the basis for competition law analysis. Thus, a strong market position within an appropriate and well-evidenced market definition assessment should constitute the key criterion. Given the diversity of online platform services, simple thresholds based on turnover, user numbers or geographic scope appear arbitrary and do not reflect the "gatekeeping" ability of a company. Therefore, the use of qualitative criteria, appears to be best to assess a potential gatekeeper position. Furthermore, the quantitative nature of the platform does not necessarily mean that problematic practices are put in place. In any case, the criteria should be clear and predictable, thus ensuring legal certainty. The currently discussed wide geographic coverage in the EU criterion appears ill-suited to identify gatekeeper platforms. Market conditions that can lead to such a position can exist across a small number or even only one single member state with the same potential risks for business users and competition. If the goal of the regulation is to protect the contestability of markets and protect business users, then this should apply anywhere where there are concerns.

Impacts of large platforms

Platforms have enabled especially small businesses to reach consumers across the single market, significantly reducing existing barriers and driving innovation. Large online platforms have created unprecedented market entry and expansion opportunities for SMEs, lowering barriers to entry, expanding their reach and enabling them to scale beyond their home market. A number of studies found that online platforms provide significant benefits for growing businesses including: market expansion, cost reduction, information expansion and price discrimination in targeting potential customers.

They also allow citizens to share and consume information across various offers and shop across borders in trusted, safe and predictable environments. The policies that platforms set for their services need to strike a careful balance of all interests involved – freedom of expression or a business user's freedom to offer products and services on the one side and societal and individual citizen interests on the other. At the same time, we are aware that there can be negative impacts and that this important task of balancing various interests will necessarily lead in some cases to unwanted effects, which should be tackled in a targeted manner. However, such concerns may appear in any online platform, irrespective of its size.

Start-ups and large platforms

The most significant factor in enabling the creation and growth of successful digital companies in Europe is a favourable investment environment, including a strong entrepreneurial foundation and a frictionless single market. A growth-oriented business policy encourages high potential entrepreneurs with the greatest potential. Factors such as support for entrepreneurs, innovation hubs, regulatory sandboxes, skills and education, as well as access to a range of different funding solutions, all play a role in encouraging start-ups and promoting their success. Competition law and other regulatory instruments protect markets and level the playing field but, by

themselves, they will not make start-ups flourish. The tech boom in the US has not been driven by stronger antitrust and regulatory regimes than those applied in Europe.

Start-ups and scale-ups naturally interact with and often benefit from larger companies, some of which are platforms while others are not. Smaller digital players use various larger online platforms or tools offered by such platforms to build new experiences and reach customers. The interrelation between larger and smaller companies is not unique to online-driven markets. The current debate unfortunately neglects the fact that platforms, no matter whether they are gatekeepers or ordinary platforms, are bringing together various types of business and consumers and therefore have incentives to see them succeed. Multi-sided markets above all mean there is a multi-sided dependency as well as symbiosis between all players. New regulation in that field may in fact reduce the innovation capacity of large platforms and thus reduce ability to empower small businesses growing and expanding into new markets.

Media pluralism and large platforms

Online platforms support media pluralism by providing creators and media with new opportunities to reach their audiences and also by introducing new ways to generate revenues. User-generated content, for instance, not only allows fans to engage with music, images or videos of their favourite artists but also offers the latter another option to monetise their works. Aggregators make it possible for publishers, particularly smaller or local ones, to reach new readers which translates into more revenues either through subscription or ads.

Regulation of large platforms

There is no evidence that companies that enjoy a so far undefined gatekeeper position exhibit a disproportionately higher negative societal or economic effect and there appears to be no research to support this claim. Platforms of any size or type of business model are subject to the same legal framework as regards privacy, consumer protection and competition. New, dedicated rules would only be justified where there are disproportionate risks specific to certain service providers under clearly pre-defined conditions. The effect of existing rules, like the Platform to Business Regulation, should also be properly analysed before new legislation is considered.

Potential rules to prohibit certain practices

The current use of the term “gatekeepers” appears to comprise a very heterogeneous group of companies with significantly different business models which might (but don’t have to) raise different regulatory concerns. Outright and generalised prohibitions exhibit a high potential of regulatory failure as their effect may vastly differ from case to case. Given the multi-sided nature of online-platforms, a prohibition that may make sense in one context may have detrimental effects for consumers in other cases or be meaningless in yet other settings. For example there

are various forms and degrees of self-preferencing, some of which may be harmful – and may already run afoul of current competition rules – while others represent important pro-consumer efficiencies that would be lost in case of a blunt prohibition. Further, a prohibition of the use and combination of data across various services of the same company risks negating important effects of economies of scale. In addition, the impact on zero-price or advertising-based business models would be different from the effect on commission-based models. Case by case analysis is therefore required, taking into consideration evidence of harm, a company's specific incentives and a analysis of all sides of the market.

Potential regulatory intervention

The rules should address specific concerns in an evidence-based approach that takes into account the particularities both of the business models and of the market conditions, which means that effective and proportionate remedies will need to be defined in a dialogue between the authority and the company. Any case-by-case remedies should only be adopted after a properly evidenced and justified finding by the relevant enforcement body. The platform subject to any such remedy should be able to appeal both the finding and the remedy, and pending any such appeal the application of the remedy should be paused.

Relationship with sector-specific rules

Sector-specific rules should continue to apply and have precedence over any gatekeeper rules. Any obvious overlaps or conflicts should however be explicitly addressed in the gatekeeper regulation in order to avoid situations of legal uncertainty.

Data-related remedies

It remains unclear what is meant by "large amounts" and what "data" is in practice. Data may be personal data or transaction data. It can be individual consumer or business user data or be aggregated. It can be raw or processed data or be combined with other existing data. Data is very rarely exclusive to specific companies given business users and consumers typically use several services that collect the same or comparable data. Furthermore, data plays a different role in zero-price markets with advertising-based business models compared to cases where services are offered against remuneration. Given the lack of definitions, the complexity of types of data, use cases and markets, it is unclear how any data-related remedies could be developed to promote competition and innovation while safeguarding data protection and protection of platforms' investment in their services. Further, data related remedies focused on a particular sector of the economy only risk distorting markets. This is why the enforcement body should ensure that such remedies apply across markets rather than applying them only to certain companies thus ensuring a level playing field.

Potential regulatory body

We think there is no need for such a body. However, should such a regulatory body be considered, it should have the necessary knowledge and expertise, be based on sound and evidence-based decision making, comprising all fair hearing rights, due process and full rights of appeal to a higher court. It should be independent and accountable. Duplication with existing regulatory enforcement bodies should also be avoided.

At a minimum the enforcement mechanism should be at EU level to ensure there are no distortions of the single market and potential inconsistencies in application across member states. It should ensure legal certainty and a level playing field across the EU. Incoherent enforcement could negatively impact competition and pose significant barriers to the Internal Market.

Tools to facilitate regulatory oversight

Investigation and monitoring are the appropriate mechanism and there already exist well-tested investigative systems based on competition law, which is the most appropriate model in this instance. Depending on the definition of 'intention to expand activities' reporting obligation, this could lead to very burdensome reporting. Online platforms continuously innovate by adding features in order to compete.

Proportionate reporting requirements could be considered to increase the regulators understanding of the platform economy. Any regulatory decisions should be based on evidence.

FOR MORE INFORMATION, PLEASE CONTACT:

Hugh Kirk

Policy Manager

hugh.kirk@digitaleurope.org / +32 490 11 69 46

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, Facebook, Fujitsu, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Qualcomm, Red Hat, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK