DIGITALEUROPE

4 MAY 2020

Towards a more responsible and innovative internet - Digital Services Act position paper

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

Introduction

The E-Commerce Directive (ECD), the legal cornerstone of Internet regulation, has brought real social and economic benefits to Europe. Indeed, two decades on from its adoption, many of the principles enshrined in the ECD remain fundamental to the functioning of the online economy. The regime has allowed the internet to grow to the size it is today, as well as encouraging innovation and creativity, from which we have all benefitted. At the same time, a result of this huge growth has also been the proliferation of illegal and harmful content online, such as hate speech or counterfeited goods which has caused real societal and economic damage. DIGITALEUROPE fully supports the need to address this in a meaningful way.

In this paper, DIGITALEUROPE proposes some fundamental principles which should inform the EU institutions as they develop their proposal for a Digital Services Act.

Country of origin

The principle of 'country of origin', which allows companies to operate seamlessly across all Member States, has been fundamental for the development of the internal market and the facilitation of cross-border trade. Maintaining the principle allows innovative ideas to scale and spread across Europe and ensure that European consumers and (especially small and medium-sized) enterprises across the 27 Member States can reap the benefits of digitisation. It should be ensured that providers of online services are subject to the law of the Member State in which they are established and not the law of the Member States where the service is accessible. This provides legal certainty for all stakeholders.

The country of origin principle remains a key element of the construction of freedom to provide information society services. DIGITALEUROPE strongly supports retaining and strengthening the principle whilst maintaining the right of a party to seek redress in a dispute in accordance with Brussels I, other specific instruments such as the Trade Marks Regulation, and recent case law developments.[1]

[1] Both the EU Regulation No.1215/2012, often referred to as "Brussels I" and Council Regulation (EC) No.207/2009 ("the Trade Mark Regulation") contain exceptions that allow a party to choose either to sue a defendant in the country of origin or in the country of destination based on rules elaborated in case law such as the recent ECJ decision C-172/18 AMS Neve Ltd.

Limited Liability

The Internet landscape has changed significantly since the adoption of the E-Commerce Directive but DIGITALEUROPE strongly believes that the principle of limited liability remains valid and strongly supports its retention.

The ECD established that online intermediaries cannot be held liable for their user's wrongdoings as long as they act expeditiously when they have actual knowledge of specific infringements. Over the years, the ECD's limited secondary liability exemptions for online intermediaries have been essential to the development of an innovative Internet economy in Europe and the protection of freedom of expression. A strict liability regime holding platforms liable would have prevented a whole range of innovative services from entering the market and would have resulted in over-removal of content. Given its importance for the functioning of the Internet, the defences contained in the ECD should be preserved 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.

Where policy requires that online intermediaries intervene to suppress content, this should be addressed through complementary statutory obligations or co-regulatory initiatives, and not by creating derogations to the liability protection in the DSA.

No general monitoring obligations

The ECD applies horizontally to various domains and any kind of illegal or infringing content. Member States may not impose a general obligation to systematically monitor information that intermediary service providers transmit or store. In addition, Member States cannot introduce a general obligation to actively look for facts or circumstances indicating illegal activity. DIGITALEUROPE strongly supports retaining this principle in the DSA.

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.

Voluntary measures clause

Although 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 such activities on their own. Some service providers perform certain voluntary monitoring activities at the moment in order to enforce their terms of service or 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.

Improving notice & takedown

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 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 might be desirable to establish the minimum information needed for a notice to be actionable (such as unique URL, 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.

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.

Horizontal framework

The ECD is a horizontal framework that applies to all information society services. It provides a horizontal liability regime for the three specifically enumerated types of intermediary service activities, provided they meet certain criteria. The intermediary service providers will be exempted from all liability for all types of activities initiated by third parties. Any statutory obligation to remove illegal third-party content should apply horizontally to any other type of illegal content. Different procedures for different types of content should only be justified by objective distinctions. A horizontal approach towards removing third party illegal content should always be the preferred option. If this is not possible, legal coherence between new vertical legislation and existing horizontal and vertical laws should be ensured, in order to avoid regulatory fragmentation.

Illegal vs harmful

The Digital Services Act should clearly distinguish between illegal[2], and lawful but potentially harmful content. Harmful content is contextual, difficult to define, maybe 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 specific vertical measures to tackle harm.

At the same time, 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.

Transparency

Improving transparency online will increase users' trust in the Internet and help foster Europe's vision for 'human-centric' digital services. The principle of transparency touches upon many different elements of discussion around the Digital Services Act. In all cases, it is important to consider the desired outcome from such transparency and intended audience (law enforcement, users, etc.) to ensure proportionality.

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 or otherwise harmful; such transparency is an essential component of platforms' accountability to their users. At the same time,

[2] No distinction should be made between civil and criminal law.

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.

There are also discussions around algorithmic transparency - the principle that the factors that influence the decisions made by algorithms should be visible, or transparent, to the people who use, regulate, and are affected by systems that employ those algorithms. 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'. The recently revised Consumer Rights Directive and the Platform to Business Regulation have already introduced proportionate obligations for online marketplaces in this regard.

Some stakeholders have also proposed introducing 'know your customer/user' obligations to the Digital Services Act. Basic verification of business identities can be useful to reduce the prevalence of counterfeits and other fraudulent activities, disincentivise bad actors online and aide law enforcement. The introduction of such obligations should, however, be proportionate and include appropriate safeguards to protect the privacy of users in the course of legitimate and lawful activities.

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, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, 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., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Qualcomm, Red Hat, Ricoh Europe PLC, 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
Bulgaria: BAIT
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN
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: Nederland ICT, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK