ASSOCIATION OF COMMERCIAL TELEVISION IN EUROPE

POSITION PAPER ON THE DIGITAL SERVICES ACT

EC PROPOSAL FOR A REGULATION ON A SINGLE MARKET FOR DIGITAL SERVICES

MEMBERS & PURPOSE - ASSOCIATION OF COMMERCIAL TELEVISION IN EUROPE (ACT)

ACT member companies finance, produce, promote and distribute content and services benefiting millions of Europeans across all platforms. At ACT we believe that the healthy and sustainable commercial broadcasting sector has an important role to play in Europe's economy, society and cultures. Commercial broadcasters are at the heart of Europe's media landscape as producers and distributors of European original content and news. We embrace the digital environment providing new services, formats and content to meet the growing European demand for quality content on various distribution models.

FACTS & FIGURES – TV IN EUROPE (ACT)

INITIAL REMARKS

The DSA addresses issues and areas Broadcasters are faced with on a daily basis, as players that stand at the nexus of media, technology, news and data policy. The DSA has a specific media dimension. ACT stresses the importance of seeing these proposals in light of fostering pluralism, safeguarding the rule of law whilst delivering innovative digital services, quality entertainment and trusted news.

The guiding mantra to benchmark the DSA - to ensure that **what is illegal offline should be illegal online** – requires to be further and fully reflected in the text and discussions amongst co-legislators. This is at the core of broadcasters view on the proposals to achieve an **effective level playing field for creative industries and viewer protections**.

Broadcasters and **media pluralism at large requires a strong liability regime** that can deliver a safe online and trustworthy environment, effective enforcement as well as ensuring that the Internet continues to fulfil its role as the vibrant and engaging place we all enjoy. While some players can continue benefiting from liability exemptions, the **DSA should not by any means grant additional liability privileges**.

The proposed regulation should reflect the present realities of the market, where several players have emerged that have surpassed "mere technical, automatic and passive nature" status.

Enlarging the **liability exemptions** to accommodate this new type of intermediaries will prove **detrimental to the content creation market** which needs more robust instruments to fight against the illegal dissemination of their content online and would fall short of answering market demand.

The proposed **notice and action procedures** will have to be analysed in light of existing copyright laws to ensure processes that lead to **rapid take down and stay down measures** can continue to be applied and improved.

Co-legislators may wish to assess lost opportunities to **crack down on online TV piracy**. The role and scope of trusted flaggers and Know Your Business Customer provisions are too narrow to effectively target and suspend abusive behaviour. Unless more is done in this respect, the broadcasting industry will suffer from online piracy for many years to come.

Similarly, there is no logical reason for **digital platforms** to **avoid liability for advertising content** which they select, place, promote and ultimately profit from. An effective regime should ensure that digital platforms are directly liable for all advertising content on their services and are held to account for content that falls short of generally accepted standards – as is the case for broadcasters.

We welcome the proposal's ability to **achieve more accountability regarding harmful content**, particularly as regards disinformation. Stringent codes of conduct will be required to **achieve tangible and verifiable results, commitments and oversight**. Mandatory independent audits imposed on very large platforms – essential to assess if these platforms effectively fight against illegal/harmful content and protect fundamental freedoms online – is a first, but not sufficient, step towards **much greater and needed algorithmic transparency**. In sum, while certain measures are in line with the needs of media pluralism and cultural sovereignty in Europe, others **will need to be revised to ensure the DSA presents a real upgrade for Europe's media ecosystem**.

ACT and members look forward to engaging with European institutions on both of these proposals. The diagnosis delivered by the EC is accurate. Now we must make sure the cure is effective. We will continue to advocate for **fair competition and a liability landscape that is fit for the digital age** in order to drive Europe's media strategy and support a robust, responsible and reliable media landscape.

EXECUTIVE SUMMARY - KEY AREAS OF FOCUS FOR BROADCASTERS

SECTION I: CONDITIONAL LIABILITY EXEMPTIONS (Chapter II, Articles 3-9)

1.1. Active/Passive distinction (Articles 3-5; 18, 20, 23)

- The requalification of articles 3-5 of the eCommerce Directive creates ambiguity and needs to better reflect the rich jurisprudence of the CJEU and national courtsOnline intermediaries that take active measures to maximise profit and consumer attention should be held liable based on criteria "optimising the presentation or promoting the content" in line with CJEU case law (L'Oréal/eBay) regardless of size
- No special regime for small players (small broadcasters have no such benefits

1.2. Ensuring that the due diligence obligations capture the right players

- Some actors play a strategic role in the piracy ecosystem and could, through their actions, contribute to limiting the phenomenon: providers of dedicated server services/leasing servers facilitate piracy by allowing hosting solutions of illegal streaming sites; providers of "reverse proxy" services are an essential link in the web woven by pirate sites to organize their anonymity
- To be fully effective, the DSA should permit the technical intermediaries mentioned above to be expressly qualified as hosting service providers under Section 2(f) of the DSA. The same reasons underlie the need to include CDN services in the definition of hosting: these are services that are increasingly being used by operators of online platforms that are clearly and almost exclusively dedicated to the distribution of counterfeit products

1.3. Make the exemption of liability conditional on the compliance with due diligence obligations (Article 5; Recital 18)

- Mandatory compliance with due diligence obligations should be a necessary precondition of eligibility for liability exemptions

1.4. "Good Samaritan" Principle (Article 6)

- "Good Samaritan" principle goes against established EU doctrine and will create a weaker system to the detriment of the European interest and online safety of European citizens; legislators should refrain from creating new liability exemptions
- The basis for the Good Samaritan – removing alleged disincentives for platforms to proactively act against illegal content – is not supported by any factual evidence and disregards already applicable duties of care on passive hosts in the eCommerce Directive
- It is not acceptable for online intermediaries to decide by themselves which kind of illegal content they intend to track or not track

1.5. Orders to act against illegal content/ Catalogue wide injunctions (Article 8; Recitals 29-30)

- Preserving the standing of national orders is important, yet Member States need greater standing to issue injunctions
- Both the applicable DSA recital and 2017 Communication do not elaborate practical basis to tackle new forms of piracy such as illegal IPTV and illegal live streaming
- DSA Article should reflect practical arrangements to terminate or prevent an infringement allowing courts to issue forward looking, catalogue-wide and dynamic injunctions

1.6. Orders to provide information (Article 9; Recitals 31-33)

- To ensure information requests are effective, the language provided in Article 15.2 (ECD) should be mirrored in Art. 9 of the DSA ;namely requests by competent authorities enabling the identification of recipients of their service with whom information society service providers have storage agreements
- It is essential that the scope of these articles is explicitly limited to cross-border orders in order to avoid unnecessary overregulation and interference in Member States' judicial laws

1.7. Content moderation (Article 12; Recital 38)

- We welcome the introduction of an obligation for all providers of intermediary services to clearly describe in their terms and conditions and to enforce in a diligent manner any policies, procedures, measures and tools used for the purpose of content moderation and recommender systems

SECTION II: DUE DILLIGENCE OBLIGATIONS FOR A TRANSPARENT & SAFE ONLINE ENVIRONMENT (Chapter III)

2.1 Notice and Action Procedures (Articles 5,14; Recitals 40,42)

- In practice, broadcasters face organisations that tend to escape their expeditious removal obligations; ACT suggests to expand the definition of the hosting services providers and simplify procedures
- Requirements proposed diminish the nature and effectiveness of the existing notice & take down procedures and need futureproofing to ensure they are not obsolete upon publication
- The title of the copyrighted content and the logo of the broadcaster are and should remain sufficient to trigger the validity of the notice as already validated by rulings

2.2 Trusted flaggers (Article 15,19; Recital 46)

- Trusted flagger system should become a standard for all hosting service providers; exclusion of micro and small enterprises misses sources of specific, prevalent and damaging types of pirated content
- The status should be refined in the proposal to recognise that the scope of entities needs to be wider than collective interests to allow for IP rightholders and their partners to effectively tackle illegal use of their content and continue to rely and develop existing best practices
- An obligation for hosting providers to treat notices from trusted flaggers with priority – and immediately for live content – should be combined with a fast track take-down procedure

2.3 Repeat infringer policy (Article 20; Recital 47)

- Repeat infringer counter-measures are welcome and to be effective need to capture micro & small entities hosting repeat infringers
- Account suspension duration (for *a reasonable period of time*) would benefit from specifications to avoid disparities in interpretations and subsequent transpositions
- The scope of suspensive measures should be widened to tackle the network of online and dynamic pirate accounts with stay down measures and termination of service for repeat infringers across all accounts
- Illegal content repeatedly uploaded should stay down

2.4 Know Your Business Customer (Article 22 NEW; Recitals 48-50)

- KYBC obligations should apply to providers of information society services that piracy services and other illegal operators rely on
- Requiring commercial entities to reveal their identity on the internet would automatically reduce illegal or harmful content online

2.5 Transparency reporting obligations for providers for online platforms & online advertising (Articles 13, 16, 23-24)

- There should not be any distinction between illegal content and manifestly illegal content
- The compliance with the due diligence obligations for a transparent and safe online environment should not be seen as burdensome
- Adapting the reach of the law to only parts of the market (digital SMEs structurally advantaged vs physical SMEs), sets a dangerous precedent and should be avoided

SECTION III: ADDITIONAL OBLIGATIONS FOR VERY LARGE ONLINE PLATFORMS TO MANAGE SYSTEMIC RISKS FOR ILLEGAL AND HARMFUL CONTENT

3.1. Risk assessment (Article 26)

- Threshold foreseen by the Commission to qualify risk as (significantly) systemic are high. The assessment should be made in light of the prejudicial nature it has on a certain sector.
- The dissemination of illegal content, infringing property rights - fully protected by Article 17 of the Charter of Fundamental Rights - should be considered as a sufficiently prejudicial risk
- Safeguards are required to preserve media integrity and avoid oversight role over broadcasters' pre-vetted and regulated content

3.2. Mitigation of risks (Article 27; Recitals 56-58)

- Regulators should have a greater role and means to compel commitments, voluntary "Codes of Conducts" and "Crisis protocols" should be more robust to qualify as effective mitigation measures

3.3. Transparency measures for very large online platforms (Articles 28-29)

- Content providers should be informed, ideally in advance, about any modification to the algorithm and the foreseen consequences on the visibility of third party content

3.4. Additional online advertising transparency (Article 30)

- We welcome the obligations as foreseen in Art. 24 and 30 as the very large online platforms monetize their business through online advertising. These obligations would help creating a trusted and transparent online environment. Broadcasters already comply with a comprehensive set of legal and self-regulatory rules [for their online and offline offerings]. Personalized advertising, which meets the same high standards, is an increasingly crucial source of revenue for media companies that don't have the reach and massive data collection of the dominant online platforms.
- Meaningful transparency measures require verifiability and open data access for regulators
- To fully assess flows of illegal/harmful content on ad networks a self-declarative approach cannot be a substitute for independent oversight and national regulatory approaches

3.5. Data access and scrutiny (Article 31; Recital 64)

- Supervision of VLOP's recommendation and moderation algorithms upon request of the Digital Services Coordinator to address pro illegal or harmful content biases should be the norm
- Princle of compliance should prevail over trade secrets to prevent the dissemination of illegal content online
- Trade secrets shall not be opposed by VLOPs to the Digital Services Coordinator, and obligations like explainability, transparency by design and active collaboration with the Digital Services Coordinator (DSC) on algorithms' purposes should be included in DSA
- DSC should be entitled to have access to all data and algorithms requested for their investigation to ensure that VLOPs are DSA compliant. Vetted researchers should be able to conduct studies on the DSA and thus require data to the VLOPs.

3.6. Codes of conducts (Article 35; Recitals 67-68)

- To deliver a true regulatory backstop, the DSA will need to be bolstered with complementary measures
- For harmful content, and associated Code of Practice on online disinformation, there is a pressing need for guidance that delivers a step change in commitments and allows regulators powers to compel a platform to adhere in good faith to a high standard co-regulatory framework, with binding commitments and enforcement with penalties

SECTION IV: IMPLEMENTATION, COOPERATION, SANCTIONS AND ENFORCEMENT (CHAPTER IV)

- The viral spread of illegal and harmful content has dramatic impact and needs immediate attention, procedures need to be streamlined to ensure the Commission can take the lead
- Relevant authorities should have the power to request and suggest commitments by VLOPs

SECTION I: CONDITIONAL LIABILITY EXEMPTIONS (Chapter II, Articles 3-9)

1.1 Active/Passive distinction (Articles 3-5)

Jurisprudence. ACT has always stressed the need for maintaining the crucial distinction between active/passive intermediaries and update it in light of CJEU jurisprudence[1]. The rich jurisprudence of the CJEU and national courts is not reflected in the approach to the conditional exemption of liability for online intermediaries.

Online intermediaries that take active measures to maximise profit and consumer attention by designing their algorithms to index and recommend content for commercial gains, play an active role and should be held liable for the content they disseminate. The optimisation of illegal and harmful content drives massive advertising revenues for these services. This is further evidence of the fact that they are not neutral nor passive vis-a-vis the content that is made available and augmented on their platforms.

ECD/Requalification of active/passive distinction. While the definition of "mere conduit", "caching" and "hosting services" (Art. 3-5) are largely similar to the provisions of the eCommerce Directive, the active/passive distinction is *de facto* requalified as active/neutral (Recitals 18, 20 and 23). This requalification creates ambiguity despite attempting to provide more clarity on the basis of the active/passive distinction, especially as set out in Recital 18 ("*the provider of intermediary services who plays an active role of such a kind as to give it knowledge of, or control over, that information")*. An intermediary that takes an editorial decision over content should not benefit from the liability limitations.

Key criteria for effective liability & scope. The key criteria for liability is and should remain "*optimising the presentation or promoting the content*" (regardless of whether this happens in an automated way or not) in line with CJEU case law (L'Oréal/eBay). We would also caution against the concept of "*deliberate collaboration*" (see Recital 20) which is a too high threshold and appears difficult to prove in practice. The criteria of "*engaging in*" is more suitable.

While we understand the need to avoid a one-size-fits-all approach, the DSA should tackle rogue players regardless of their size. Size cannot be a criteria for existing rules. Exemptions for small players are exclusively provided for online intermediaries. Small broadcasters do not benefit from the same exceptions, and we as such encourage policy-makers to not adopt a two-tier approach to the law by allowing small rogue players to continue their illegal activities in a legal vacuum. Any new classification should uphold the EU *acquis*[2].

1.2. Ensuring that the due diligence obligations capture the right players

Some players play a strategic role in the piracy ecosystem and could, through their actions, help to limit the phenomenon. This is the case inter-alia for **dedicated server / server leasing service providers** which could facilitate piracy by allowing illegal streaming site hosting solutions to be put in place; "reverse proxy" service providers are an essential link in the spiderweb woven by pirate sites to organize their anonymity. The "reverse proxy" acts as an IP address scrambler to the rest of the Internet. Such practices provide malicious sites with an IP address that does not match that of the server on which they are hosted. Even though these intermediaries are often the only ones that rights holders are able to identify, there is uncertainty as to the liability regime applicable to them with regard to the mechanisms provided for by the DSA. To be fully effective, the DSA should make it possible to expressly qualify the technical intermediaries mentioned above

[1] www.acte.be/publication/ACT-perspectives-on-the-digital-services-act
[2] See Annex I for some relevant ECJ decisions

as hosting service providers within the meaning of Article 2 (f) of the DSA. The same reasons underlie the need to include CDN services in the definition of hosting: these are services that are increasingly being used by operators of online platforms that are clearly and almost exclusively dedicated to the distribution of counterfeit products.

Equally, other types of players which are similarly dangerous for circumventing broadcasters rights are the Virtual Private Networks (VPNs). The latter are mentioned as part of mere conduits in the Commission's Impact Assessment[3], however this is not explicitly stated in the proposal. We would therefore suggest that policy makers introduce a reference to VPNs in Recital 27 of the proposal.

1.3. Exemption from liability conditional on the compliance with due diligence obligations (Article 5a)

Conditionality. Providers of hosting services including online platforms should be deemed ineligible for the liability exemptions foreseen in Article 5. Mandatory compliance with due diligence obligations should be a precondition of eligibility for liability exemptions. This is an effective solution to ensure compliance with the Regulation. This conditional approach to liability exemptions produces more tangible results and incentives; specifically in cases where penalties foreseen could be factored in as a cost of doing business, rather than genuinely adhering to the principle of delivering a higher level of safety online and increase in consumer trust.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2020:348:FIN, Part II, page 168

1.4. "Good Samaritan" Principle (Article 6)

Legal certainty. We question the legal certainty this principle brings in comparison to clear and long established CJEU jurisprudence on "active hosts", clearly indicating that intermediaries optimising content do not have a neutral position and are therefore not entitled to the privileges of liability exemptions. The so-called "Good Samaritan" (GS) principle would only benefit certain large online platforms rather than the European interest or a safer online space.

Established jurisprudence. The GS principle goes against established EU doctrine and risks being abused by active platforms looking to avoid liability entirely. Without a strong safeguard this will create a weaker system. Liability of active hosting platforms needs to be bolstered, not watered down. Article 6 introduces the concept of removing alleged disincentives for platforms to proactively act against illegal content. Yet there is no evidence to support the existence of said alleged disincentives. Moreover, the assumption that platforms need protections to avoid losing their "passive host" status, fails to recognise that duties of care are already applicable to passive hosts in the eCommerce Directive (Recitals 40, 48).

Perverse incentives. The principle creates a perverse incentive for active hosting platforms to requalify themselves in order to ensure they are shielded from liability. The EU needs to strengthen its tools to ensure that citizens in the EU are afforded a high level of protection, alongside being well informed from a plurality of perspectives. Without safeguards, online intermediaries will always be impermeable to CJEU caselaw and will never be requalified as active and fully liable. Allowing online intermediaries to decide for themselves the type of illegal content they choose to track or not may not necessarily align with effective prioritisation of illegal and harmful content which negatively impact EU citizens.

1.5. Orders to act against illegal content/Catalogue-wide and dynamic injunctions (Article 8)

Reinforce legal basis. It is of the utmost importance that judicial or administrative authorities may bolster their courts' ability to issue forward looking, catalogue-wide and agile injunctions. This allows for effective tackling of new forms of IP infringements, such as illegal internet protocol television (IPTV) and other forms of illegal (live) streaming. As of today, the EU Commission only advocates[4] that such measures are not contrary to Article 11 of the Directive[5]. The proposed regulation on the DSA, only recalls in its recitals that the liability regime does not affect the possibility for a court or administrative authority, to issue injunction to terminate or prevent an infringement (Recital 24). This is not sufficient. In some Member States, such as France, Courts remain reluctant to issue such injunctions without a greater legal basis to buttress their opinion.

Scope. Orders to act usually don't focus on a specific item but rather on the domain names of the platforms via which the illegal content is made available. The order usually aims at disabling access to a website or blocking IP addresses. Also, the exact uniform resource locators (URLs) can't be deemed necessary to identify the illegal material on a platform service. Furthermore, the requirement to have the order drafted in the language of the provider risks slowing down the process. Relevant national judicial or administrative authorities should be allowed to send orders in their national languages.

[4] 2017 Communication intended to provide guidance on the enforcement of the IPRED Directive – link
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004L0048R(01)

1.6. Orders to provide information (Article 9)

Scope of information reflecting practices. The collection of information should be extended beyond information already obtained by the provider in order to avoid jeopardising the effectiveness of the provision and conflict with the practices currently carried out under the e-Commerce Directive. Article 15.2 ECD already allows providers to collect information that effectively enables the identification of the recipient of the service[6]. To ensure information requests are effective, the language provided in Article 15.2 of the ECD should be mirrored in Art. 9 of the DSA.

Scope limitation to cross-border orders. The clear intention of Articles 8 and 9 is to harmonise aspects of orders that are of a cross-border nature. This is however not explicitly reflected in the current wording of the articles; which seem to capture all orders, regardless of their territorial scope. It is essential that the scope of these articles is explicitly limited to cross-border orders in order to avoid unnecessary overregulation and interference in Member States' judicial laws. This limitation is therefore necessary to ensure remedies that currently exist under national law (often by virtue of EU norms) are not undermined.

1.7. Content moderation

Recommendation tools and content moderation (or lack thereof) are largely to blame for the spread of illegal and harmful content online. However, they can be part of the solution to address it.

We therefore welcome the introduction in Article 12 of an obligation for all providers of intermediary services to clearly describe in their terms and conditions and to enforce in a diligent manner any policies, procedures, measures and tools used for the purpose of content moderation and recommender systems.

This should include explicit references to how content that is illegal or has the potential to harm users, such as the spread of disinformation, discriminatory content or content that harms minors. In this respect, to publicly know which tools are used to moderate content is not sufficient to understand if algorithms designed by very large online platforms contain biases that promote illegal or harmful content.

Very large online platforms as defined by Article 25 of this Regulation shall not have lawfully uploaded content owned, and editorially selected by an audiovisual media provider as defined in Article 1 Paragraph 1 (a) in the AVMS Directive (2018/1808) unduly obscured, obfuscated or otherwise disabled by virtue of its alleged non-adherence to terms and conditions that go beyond the thresholds applied to legal and harmful requirements applicable in relevant European and national regulations and jurisdictions (see point 3.1.).

[6] "2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements".

SECTION II: DUE DILIGENCE OBLIGATIONS FOR A TRANSPARENT AND SAFE ONLINE ENVIRONMENT (Chapter III, Section 2, 3, Articles 14-24)

2.1 Notice and Action Procedures (Article 14)

Broadcasters need robust and effective instruments with high liability standards for the protection of content on all online service providers. As a whole, the procedures described in the Commission's proposal are limited to hosting providers and are overly burdensome to achieve the desired outcomes.

Extension of definition of hosting provider. In practice, broadcasters face organisations that tend to escape their expeditious removal obligations, manipulating their business model in order to argue that they qualify as mere infrastructure providers. This is particularly the case for organisations that do not only provide a web hosting service but also a server leasing service, allowing their customers to offer hosting services to their own subscribers. In order to make sure that such organisations comply with the obligation provided for hosting service providers - namely Article 14 of the DSA Proposal (ie. Notice and Action) - we suggest to adjust the definition of the hosting services providers set forth in Articles 2 and 5 to include the leasing of servers for hosting services.

Content of notices. The title of the copyrighted content and the logo of the broadcaster are and should remain sufficient to trigger the validity of the notice as already validated by rulings[7]. Any other more time-consuming requirements are unwarranted and go against the established EU acquis. As such we recommend that a number of clarifying amendments be made to Article 14.

The requirements of the notices which include an explanation of reasons as to why notified content is considered illegal, a statement of good faith, exact URL or URLs, and where necessary additional information enabling the identification of the illegal content (Article 14.2.(b)) are costly and time consuming. The notice and action requirements proposed will diminish the nature and effectiveness of the existing notice and take down procedures, which are already ineffective in respect of content (e.g. live sport) where expeditious take down is a necessity. The requirement to provide for a URL is especially problematic for structurally infringing platforms, particularly as it is not coupled with a robust stay-down obligation.

The systematic re-uploading, for example under a different URL, of content reported as illegal significantly undermines the effectiveness of notice and action systems and has a negative impact on media companies which have to issue multiple takedown requests for the same or similar illegal content. It is a clear signal that the system is being abused. In addition, it is sometimes impossible to extract an URL for an infringing video. The requirement to provide for a URL does not allow for technical innovations or changes. The current wording does not provide for a future proof solution and risks to become obsolete immediately after publication.

2.2 Trusted flaggers (Art. 19)

Scope. The Commission's decision to exclude from the scope of Chapter III, micro and small enterprises, does not account for the damaging role that such small platforms can play on specific types of pirated content. We firmly believe that ensuring that what is illegal offline is illegal online is dependent on a certain equality in

[7] RTI vs Dailymotion – Ruling of the Court of Rome of 15 July 2019; RTI vs Yahoo – Ruling of the Italian Supreme Court (Corte di Cassazione) of 19 March 2019; RTI vs. Facebook: Ruling of the Court of Rome of 15 February 2019; TI vs VIMEO: Ruling of the Court of Rome of 10 January 2019

front of the law regardless of size. ACT believes that the trusted flagger system should become a standard for all hosting service providers.

Attribution. ACT is a strong advocate for IP rightholders and their partners to be recognised as trusted flaggers. We welcome the Commission's proposal to formalise the attribution of such a quality by involving an independent third party (the Digital Services Coordinators), but based on established practices, hosting services should also continue to be able to appoint trusted flaggers. Indeed, some have similar systems in place and collaboration can work. Shifting attribution entirely to DSCs would slow the process down.

Moreover, we are concerned with the requirement that the trusted flagger should represent collective interests in Art. 19.2(b). Such a provision would not qualify our members (and third parties operating notices on their behalf) as trusted flaggers although they have been at the forefront of the evolution of notice and action mechanisms and have invested to develop them. This is a retrograde step from the position today and should be corrected. It is imperative that broadcasters be clearly included so as to preserve their IPR commitments and uphold their rights.

Expediency. ACT has insists that the content flagged by trusted flaggers should always trigger a fast track procedure. Whilst the Commission's proposal has the potential to provide with a helpful instrument for the industry, we believe that an obligation for hosting providers to treat notices from trusted flaggers with priority should be combined with a fast track procedure if it is to be effective in the fight against illegal content in a fast paced online environment. As regards infringing live content, when notified by trusted flaggers, the infringing content should be removed immediately.

To this end, we recommend that a number of clarifying amendments be made to Article 15 and respectfully suggest moving Article 19 from Section 3 of Chapter III, to Section 2 of Chapter III in combination with slight alterations for the instrument to become an effective instrument for broadcasters to fight against online piracy.

2.3 Repeat infringer policy (Article 20)

Scope. ACT welcomes the European Commission's intention to provide legal certainty regarding repeat infringers. We however believe that proportionality in this case is not best served with obligations limited to online platforms and very large online platforms; while dissuasive measure would not apply to micro and small enterprises. For more efficiency in the fight against infringers, we suggest moving Article 20 from Section 3 of Chapter III, to Section 2 of Chapter III.

Timing of suspension. Equally, the prospect of suspending the repeat infringing accounts for a reasonable period of time does not constitute a sufficient safeguard in light of the systemic nature of online piracy because it is very easy for users to create new accounts and repeat infringing behaviour. Article 20 should clarify that, just as illegal content repeatedly uploaded should stay down, hosting services should terminate the provision of their services to recipients that frequently provide illegal content, regardless of which account they use to access the service. A small proportion of hosting services already have similar systems in place that work. This should equally be the case for recipients of service that facilitate the dissemination of illegal content.

As such we recommend that a number of clarifying amendments be made to Article 20.

2.4 Know Your Business Costumer (KYBC) (Art. 22)

Scope. The Commission has proposed the underlying idea of the KYBC in providing for rules requiring platforms to know the identities of traders using their services to promote messages or offer products or services to EU consumers (see Art. 22 and Recital 49). Unfortunately, the scope of the KYBC provision is too narrow, as it is limited to online platforms which allow "consumers to conclude distance contract with traders", i.e. marketplaces, thereby excluding infrastructure services. As a result, it fails to provide meaningful assistance in fighting illegal websites and audio-visual streaming services that contract for the use of such services. KYBC obligations should apply to providers of information society services that piracy services and other illegal operators rely on. Requiring any commercial entity to reveal its identity on the Internet would automatically reduce illegal or harmful content online. Limiting KYBC to online marketplaces is a missed opportunity to address the broad range of illegal content online.

In order to ensure that KYBC provisions can meaningfully contribute to the goal of creating a safe and predictable online environment for European citizens and legitimate European companies, the scope of application should be broadened to cover all providers of intermediary services. We therefore suggest an amendment to Article 2 to include a definition of "business customers" that would make a clear distinction between commercial operators and private customers (who would be out of scope) and put in place safeguards to ensure full compliance with existing EU acquis.

On the KYBC provision, we respectfully invite policy makers to consider moving Article 22 to Chapter III Section 1, which would broaden its scope of application to all providers of intermediary services, including providers of infrastructure services.

2.5 Transparency reporting obligations hosting services and providers for online platforms (Articles 13, 23-24)

Scope. We welcome the basic obligations of Art. 13.1 (a), (b) and (c) as they address a real need.

Information obligations. Transparency of online platforms requires detailed information on actions taken and on the notices received, as well as on the time for processing. Confirmations of receipt should be sent to notice providers to avoid that the latter have to check manually whether his/her request has been followed through. This can also serve as evidence in judicial or out-of-court proceedings. We welcome the provisions requiring additional *transparency measures in Articles 23 - 24* for online platforms. We note the requirement in Article 23.1(b) to provide reporting for the suspensions enacted regarding manifestly illegal content. As explained above, ACT firmly believes that there should not be any distinction between illegal content and manifestly illegal content. Prohibited content is detrimental to European values, regardless of whether it is manifestly illegal or simply illegal.

Due diligence applied fairly. The compliance with the due diligence obligations for a transparent and safe online environment (particularly those pursuant Articles. 13, 19, 20 and 22) should not be seen as burdensome. Enterprises willing to be active players in the digital environment, whatever their size, should make sure that their services by design limit fraud and encourage transparency. In this respect, the regime should be proportionate yet be mindful of creating dual obligation types – namely between digital and other SMEs – on due diligence requirements. All businesses should be expected to have reliable reporting, measures against misuse, KYBC and other measures in place. Otherwise, the objectives to (i) ensure that what is illegal offline should be illegal online, and; (ii) to guarantee a safer online environment for internet users and customers; would be missed.

As such we recommend that a number of clarifying amendments be made to Article 13, 16 and 23.

SECTION III: ADDITIONAL OBLIGATIONS FOR VERY LARGE ONLINE PLATFORMS TO MANAGE SYSTEMIC RISKS FOR ILLEGAL AND HARMFUL CONTENT (CHAPTER III, SECTION 4, ART. 25-33)

3.1 Risk assessment (Article 26)

Regular assessments with meaningful oversight. We welcome the obligation for very large online platforms to conduct risk assessments specific to their services, especially with regard to illegal and harmful content. Such requirements are a step in the right direction for providing users and business users with much needed visibility with regard to content moderation systems that these platforms deploy, the systems of selecting and displaying advertising around illegal content, on one side, and harmful and intentional manipulation of their services, on the other. These assessments should be more regular.

Thresholds to be adjusted. We are concerned that the thresholds foreseen by the Commission to qualify risk as systemic or significantly systemic are quite high. We firmly believe that the dissemination of illegal content, infringing our members' property right which is fully protected by Article 17 of the Charter of Fundamental Rights of the EU, bringing substantial prejudice to our members' bottom line, should be considered as sufficiently prejudicial risks. For broadcasters, the routine distribution of infringing content is sufficiently prejudicial to imply a systemic risk. The terms that very large online platforms should take into account such as "rapid and wide" dissemination are of little consequence to broadcasters. If European legislators wish to provide rightsholders with a sufficiently robust toolbox, the systemic nature of the risk should be assessed in light of the prejudicial nature it has on a certain sector.

Very large online platforms should refrain from taking any editorial decision, in the sense of removing, suspending, disabling access to or generally interfering with pre-vetted content. Given the significant impact of such platforms on the formation of opinion in Europe and increasingly on media plurality, very large online platforms should refrain from taking any editorial decision, in the sense of removing, suspending, disabling access to or generally interfering with pre-vetted content lawfully uploaded from the account of a recognised audiovisual media provider as defined in Article 1 Paragraph 1 (a) of the AVMSD Directive (2018/1808), in order to preserve and uphold media and editorial freedom. The obligation of not interfering with curated content emanating from an audiovisual media provider should have no effect on the measures very large online platforms take to disable the dissemination of illegally uploaded content.

3.3. Mitigation of risks (Article 27)

ACT welcomes the mitigation of risks obligations for very large online platforms, and particularly Art. 27.1 (b) and (d). This could be a useful element in broadcasters' fight against online piracy and the necessary hook to switch from a self-regulatory to a co-regulatory model to tackle harmful content online.

Adequate content moderation and recommender systems. Platforms benefit directly from the spread of harmful content that they recommend and amplify (notably via their algorithms) and they should behave diligently with regards to it, as broadcasters do. Risk mitigation provision measures are an essential step in building a regulatory environment in which online platforms are responsible for the harmful content – be it legal or illegal – that they distribute and amplify through their services. Adequate content moderation and recommender systems are essential to address systemic risks foreseen in Art. 26. It would be useful to build upon this by introducing a non-exhaustive list through recitals of the different practices covered: from content

removal, amplification/de-amplification of content, artificial delays to limit virality, to the ban/suspension of accounts.

The introduction of risk mitigation measures outlined in Art. 27 is positive insofar as it will contribute to an environment where platforms have to behave responsibly. This is equally true of the possibility for the Commission and Digital Services Coordinators to issue guidelines.

Role of regulators. We are concerned about the proposal's over-reliance on voluntary "Codes of Conducts" and "Crisis protocols" to demonstrate platforms' mitigation measures. Regulators should have a more direct role in drawing up these mitigation measures and have the means to order platforms to make specific commitments (see also amendment to article 41 below).

While broadcasters are supportive of the measures in place to create more accountability for very large online platforms, another element should be taken into account. Broadcasters' content – both offline and online – is strictly regulated by national and European legislation.

At present very large online platforms can unilaterally demote Broadcasters' content if they deem it non-compliant with their policies. This comes at a great cost to media and editorial freedom especially given the platforms' influence on shaping opinions and perceptions. Co-legislators should ensure provisions address situations where platforms with so called absence of editorial responsibility take editorial decisions over content that is selected by editorially responsible entities.

This aspect also raises severe economic concerns in the online advertising market, as platforms may unilaterally remove content to damage broadcasters. To preserve the integrity of our services, the visibility of our content, and bolster competition in online advertising; very large online platforms' terms and conditions should not apply to lawfully uploaded pre-vetted content of editorially responsible players such as broadcasters. This should always be the case when the content emanates from its rightful owner, or from a legal source. However, such a ban on secondary control of content should not have any effect on the obligation of online intermediaries to act against illegal uploads of broadcasters content.

3.4. Transparency measures for very large online platforms (Articles 28 – 29)

We call for the implementation of time efficient and dynamic supervision of VLOPs' algorithms mechanisms. The lee-way afforded to platforms in Article 28.4, where operational recommendations of the independent audit are not mandatory as long as the platform can justify why it has not done so. Such a provision provides a loophole for platforms to escape responsibility and taking the prerequisite actions.

We welcome more transparency on recommender systems and their parameters (Art. 29) as a first step, but the whole VLOPs' algorithms supervision should be defined as previously explained to be really effective to fight against the dissemination of illegal and harmful content on a large scale. Supervision of VLOP's recommendation and moderation algorithms upon request of the Digital Services Coordinator to address pro illegal or harmful content biases, prevalence of compliance over trade secret to prevent the dissemination of illegal content online.

3.5. Additional online advertising transparency (Article 30)

We welcome the obligation for very large online platforms to compile and make publicly available advertising repositories (Article 30). This will aid regulators to assess the revenues made by very large online platforms

through the dissemination of illegal and harmful content and would provide advertisers with more visibility on the systems in place, helping the latter to ensure greater brand safety online.

The very large online platforms monetise their business through online advertising and have real market dominance due to their reach and massive data collection capabilities. More accountability and visibility is a prerequisite for a healthy online environment. We do however fear that the reporting on these figures will be done unilaterally by very large online platforms, once again without any regulatory or independent oversight.

Sponsored content and advertising are instrumental in monetising and amplifying the spread of harmful content on online platforms. Mandatory advertising transparency obligations as foreseen in Articles 24 and 30 are a positive development but they represent the bare minimum acceptable. Online platforms directly draw their revenues from online advertising and should be held responsible for it, as is the case for broadcasters. Where platforms suspend accounts or take-down content because of illegal activities, breach of terms and conditions or in compliance with codes of conducts, they should refund the advertisers and disclose this in their registries. The same applies to ads suspended by platforms.

It should also be noted that personalised advertising is a crucial and growing source of revenue for media companies. These targeted solutions can improve the effectiveness of advertising, increase its value, and enhance the viewer experience. The DSA creates the conditions for fair competition as it does not impose unnecessary restrictions and obligations on online advertising, which already has to comply with a comprehensive set of legal and self-regulatory rules, including regarding data and privacy.

3.6. Data access and scrutiny (Article 31)

ACT supports strong measures that would increase the accountability and transparency for very large online platforms (VLOPs), especially in light of their dual role as distributors and publishers of information. We firmly believe that shedding light on activities that have been conducted in the dark through algorithms' black boxes, will help the Digital Services Coordinators, the newly established Board and the Commission to understand the influence very large online platforms have on consumer behaviour, the way content is distributed and monetised online to maximise the profits of these players and the consequences such power holds.

Considering the major role played by VLOPs' algorithms in the acceptance, ranking and dissemination of illegal and harmful content; failing to provide a solid control and supervision mechanism on a permanent basis (given that the algorithms are constantly evolving) of algorithms related to moderation, ranking, acceleration and recommendation will make the DSA regulation miss its primary goal[8]. Transparency measures mentioned in the DSA seek to tackle the effects of the dissemination of illegal and harmful content, our proposal is focused on addressing the root causes. Algorithms are built by humans in order to capture the attention of the users on the VLOP for commercial and data collection purposes. In this way, VLOPs are encouraged to promote the most engaging content which is very often of an illegal and/or harmful nature. In practice, this means that algorithms may contain illegal or harmful content biases, voluntarily or unintentionally, which should be detected and corrected quickly by the Digital Services Coordinator.

Reciprocally, trade secrets should not be opposed by VLOPs to the Digital Services Coordinator. Obligations like explainability[9], transparency by design and active collaboration with the Digital Services Coordinator on algorithms' purposes should be included in the DSA. This kind of mechanism will be the best guarantee for EU

[8] For further reference on this, see the following study https://cdn.uclouvain.be/groups/cms-editors-crides/droit-intellectuel/CRIDES_WP_2_2021_Alain%20Strowel%20and%20Laura%20Somaini.pdf

[9] Extent to which the internal mechanics of a machine or deep learning system can be explained in human terms

citizens to be protected from illegal and harmful content. This will also ensure the respect for freedom of speech whilst ensuring this (and other fundamental rights) is not implemented at the VLOPs' sole discretion and according to its own interests. As such, if a clear editorial bias is detected, or any bias leading to the dissemination of illegal/harmful content, VLOPs should lose their liability exemption to reflect the loss of claimed neutrality. This neutrality itself can only be reasonably assessed with proper supervision of content-related algorithms.

In order to reach a proper balance between fighting against illegal and harmful content online and respecting VLOP's trade secrets, article 31 should be split in two parts. The first one addressing data access for DSCs or the Commission and the second one dealing with access to data for vetted researchers. They cannot be treated in the same way as the guarantees offered to deal with trade secrets are not alike.

DSCs should be entitled to have access to all data and algorithms requested for their investigation to ensure that VLOPs are DSA compliant. Vetted researchers should be able to conduct studies on the DSA and thus request data from the VLOPs. Yet only the DSCs (being NRAs) provide the required guarantees to handle highly sensitive data. As such, while trade secrets may be opposed to vetted researchers where warranted, the same cannot be justified for NRAs which have extensive expertise in handling trade secrets to ensure proper compliance. This is already the case for a large swathe of sectors such as telecoms, health, finance… A blanket exception granted to VLOPs on the basis of trade secrets would not be justified and would introduce a major loophole in the DSA implementation.

The transparency measures should extend to the key criteria for aggregation, selection and presentation of content, as well as functionalities of the algorithms in real time. When criteria or algorithms are modified, such changes need to be communicated immediately. Additionally, empowering the Commission to adopt standards on reporting templates is also commendable to avoid situations whereby the lack of verifiable and common key performance indicators severely undermine the monitoring and verifiability of the claims made.

3.7. Codes of conducts (Art.35)

We welcome the declaration of the Commission in its European Democracy Action Plan that the Digital Services Act would contain a co-regulatory backstop with regard to the Code of Practice on online disinformation. Creating a link between the Digital Services Act and the Code of Practice (CoP) on online disinformation through Art. 26, 27 and 35 is very important. Yet, the current text is too flexible to be considered a true regulatory backstop. In our view, for such a co-regulatory backstop to be effective, it is essential that (a) regulators have the power to compel a platform to participate in good faith in a co-regulatory framework; (b) that it be held against platforms when they do not participate in good faith, and; (c) that the code be binding and enforceable by regulators directly through fines. ,

Finally, the descriptions of the codes of practices in recitals 67 and 68 are not helpful as it does not reflect the co-regulatory nature that such codes are meant to have, particularly in the field of disinformation. Language describing disinformation should also be reinforced. We would support an enhanced role for the Board in the development of codes of conducts. As ERGA stressed in its assessment report on the Code of Practice on online disinformation[10]: "*existing backstop mechanisms are already functioning in other areas on a member state level and these tend to be grounded in EU and Member States legislation that provides for a state-founded, albeit often independent, authority*". The Board could fulfil such a role. As such we recommend that a number of clarifying amendments be made to Article 35.

[10] https://erga-online.eu/wp-content/uploads/2020/05/Executive-Summary-ERGA-2019-report-published-2020.pdf

SECTION V: IMPLEMENTATION, COOPERATION, SANCTIONS AND ENFORCEMENT (CHAPTER IV, SECTIONS 1-3)

The spread of illegal and harmful content can have swift dramatic impact (as was seen recently in France for hate speech or in the U.S. for disinformation). The lengthy procedures foreseen in the proposal before the Commission can take the lead and investigate are too lengthy and should be streamlined.

As outlined above, relevant authorities should have the power to request and suggest commitments by VLOPs in relation to their compliance with articles 26 and 27 of the DSA. As such we recommend that a number of clarifying amendments be made to Article 38, 41, 43 & 45.

ANNEX I - REFERENCES TO ECJ JURISPRUDENCE

Relevant CJEU case-law:

- "*Where, by contrast, the operator has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of or control over, the data relating to those offers for sale. It cannot then rely, in the case of those data, on the exemption from liability referred to in Article 14(1) of Directive 222/31*". (Case C-324/09 L'Oréal and others)
- "*if the fact remains that those operators, by making available and managing an online sharing platform such as that at issue in the main proceedings, intervene, with full knowledge of the consequences of their conduct, to provide access to protected works, by indexing on that platform torrent files which allow users of the platform to locate those works and to share them within the context of a peer-to-peer network. In this respect […] without the aforementioned operators making such a platform available and managing it, the works could not be shared by the user or, at the very least, sharing them on the internet would prove to be more complex*". (C-610/15 Stichting Brein v. Ziggo – The Pirate bay case)
- "*[...] user makes an act of communication to the public when he intervenes, in full knowledge of the consequences of his action, to give access to a protected work to his customers and does so, in particular, where, in the absence of that intervention, his customers would not, in principle be able to enjoy the broadcast work*" (Case C-527/15 Stichting Brein v. Filmspeler)
- "*it is to be determined whether those links are provided without the pursuit of financial gain by a person who did not know or could not reasonably have known the illegal nature of the publication of those works on that other website or whether, on the contrary, those links are provided for such a purpose, a situation in which that knowledge must be presumed*." (Case C-160/15 GS Media)