AIM EUROPEAN BRANDS ASSOCIATION

Avenue de Gaulois 9
B-1040 Brussels
Belgium
Tel: +32 2 736 0305
TR: 107438267901
www.aim.be

AIM POSITION PAPER

The EU Commission Consultation for the Digital Services Act: September 2020

8 September 2020

Table of Contents

Chapter 1: Illegal Goods, Counterfeit and Online Platforms

- **The Digital Services Act is the opportunity to introduce clear legal obligations for platforms to do more to prevent the distribution of illegal goods especially by addressing known fraudulent activities. The current voluntary/self-assessment mechanisms (also known as the "Good Samaritan" principle) are not adequate to address the increasing volume of illegal goods on platforms.**

- **Platforms should be required to verify the identity of sellers. This can be achieved by using already existing databases and anti-fraud tools. This is a key element that would at the same time discourage fraudulent sellers from accessing the platforms and help attribute liability in case of issues.**

- **The DSA should introduce transparency and data sharing obligations. Platforms should share data about infringers with authorities. Platforms should report periodically on the volume of illegal goods detected, as well as pertinent actions they have taken.**

- **Notifying illegal goods is still too burdensome due to the fragmented approach across the different platforms. While there should always be room for each platform to improve its services, a minimum set of best practices should be introduced to reduce the burden for those notifying illegal goods.**

- **Once a good is identified as illegal, it should not be possible to re-list it, and platforms should use tools to enforce their removal. Current practices mean that illegal goods are not effectively removed, but rather bounce on and off platforms.**

- **Consumers should be informed if they have purchased products that have since been delisted due to being illegal. This would allow consumers to avoid any further harm and seek redress.**

1. Brands and online platforms:

AIM represents over 2500 brand owners across the EU and beyond, covering a broad range of products[1]. One of the most important elements of a brand is bringing innovation to consumers, which can only be sustained as long as there is a fair level playing field, consumer protection and certainty.

Brands serve the needs of consumers across multiple channels both offline and online. Consumers are increasingly buying branded goods via online stores and platforms. Developing products, ensuring their distribution and trying to tackle the growing number of illegal goods, frequently sold next to legitimate goods, provides brand owners with a detailed understanding of the benefits, but also of the challenges, that come with the platform economy.

1.1 Providing consumers and businesses with a clean online platform economy:

Brands are successful on platforms and confident in the future of this channel, as long as platform operators are able to ensure a clean and safe environment by enforcing effectively preventive and proactive measures against the increasing volume of illegal goods. As illustrated by the recent crisis, consumers are exposed to a high number of fraudulent activities as criminals are exploiting the opportunities to sell illegal goods via online platforms. Without such measures, consumers and businesses will remain exposed to harm from the increasing volume of illegal goods[2]. To ensure a safe, trustworthy and clean online platform economy, the same rules that are applied offline should apply online.

1.2 Digital Services Act: EU can take the lead to enable a healthy platform economy:

The Digital Services Act is a timely initiative for the EU to take the lead by implementing the best solutions and address illegal goods sold on platforms, ensuring a future-proof legislative framework for a healthy, sustainable and thriving platform economy. We welcome the EU Commission's perspectives outlined in the Roadmap (favouring options 2 + 3) and the acknowledgement of the issues in the Consultation.

Companies of all sizes, including SMEs, are currently investing significant resources into monitoring and notifying platforms of illegal goods. Investing resources that could be better used elsewhere into searching for illegal products on platforms could be avoided if all parties played their part.

The entire value chain, including consumers, needs an effective legal framework to guard against the numerous infringements of consumer and business rights. The future system should be balanced, providing stakeholders with clear and measurable guidelines around their obligations as well as an efficient enforcement mechanism to combat lack of compliance. The updated legal framework should ensure that rules are effectively enforced regarding illegal goods, online and offline – as stressed in the Commission's 2017 Communication and its February 2020 Communication on shaping Europe's digital future: "*What is illegal offline is also illegal online*".

This will be achieved only if the future framework requires compliance and the proactive fight against illegal products, providing all platforms, big and small, with legal certainty and equal opportunities to develop and be successful in the internal market.

[1] For a detailed overview of the AIM National Associations and Corporate Members please visit the AIM website here https://www.aim.be/members/

[2] **Europol 27 March 2020, PANDEMIC PROFITEERING: HOW CRIMINALS EXPLOIT THE COVID-19 CRISIS** https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

Similarly, other countries are tackling these challenges and strengthening their measures to prevent the sale of illegal goods online (e.g. US Report on Combating Trafficking in Counterfeit and Pirated Goods; Executive Order on Ensuring Safe & Lawful e-Commerce for US Consumers, Businesses, Government, Supply and IP Rights; the Shop Safe Act 2020)[3].

2. Illegal goods and online platforms

The volume of illegal goods reaching consumers, including via online platforms, is increasing[4]. There are several studies and coordinated test purchase experiments[5] demonstrating the fact that the current approach taken by platforms is no longer sufficient and a legal framework requiring a preventive and proactive approach in the form of legally binding obligations is necessary to address effectively the flood of illegal products being offered to consumers online.

Brands, law enforcement authorities, retailers, platforms, payment providers, fulfilment and transportation companies, and others in the supply chain, all have a responsibility to prevent illegal goods reaching consumers. As online platforms play a key role in preventing fraudsters from abusing consumers, the new legal framework should introduce measures to require that platforms must prevent illegal products from being offered to consumers. Multiple solutions and tools could also be used more broadly and more systematically and should be considered as being part of doing normal business as they aim at protecting consumers, for instance screening for rogue traders and illegal products (more details in section 3 and in the annexes).

2.1 The current Good Samaritan principle is inadequate:

The Good Samaritan principle is to be understood as platforms acting on a voluntary basis as neutral bystanders, deciding what the necessary measures should be. It is a voluntary and self-assessment system which leads to a fragmented and inadequate set of actions against illegal goods. In the view of most stakeholders this is an outdated perspective of the role of platforms. This voluntary/self-assessment approach has resulted in legal uncertainty and a high volume of illegal goods transiting platforms, harming both consumers and businesses. The DSA should introduce clear positive legal obligations that bring legal certainty and address the known issues around illegal goods and platforms.

2.2 The main challenge: it is too easy to sell illegal goods on online platforms:

Illegal goods are dangerous to consumers and have a major negative effect on the economy and the level of consumer trust. Consumers and businesses are increasingly using platforms for all their needs. The volume of illegal goods sold on platforms continues to increase and platform operators should be required to ensure their environment is clean, competitive and safe. Consumers are misled into buying dangerous and fake goods, often left feeling cheated. The 2016 Global Consumer Shopping Habits Survey[6] revealed that almost one

[3] https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf
https://www.whitehouse.gov/presidential-actions/ensuring-safe-lawful-e-commerce-us-consumers-businesses-government-supply-chains-intellectual-property-rights/
https://www.congress.gov/bill/116th-congress/house-bill/6058/text?r=3&s=1

[4] According the OECD and EUIPO, counterfeit and pirate goods account for 3.3% of global trade and up to 6.8% of all imports by value to the EU. The boom in fakes comes as technology makes it easier to buy and sell goods online, with the report highlighting "*digital platforms which help connect supply and demand globally*" as having a particular impact. The EUIPO also found that in 2013-2017, the presence of counterfeits in the EU marketplace caused the loss of over 670 000 jobs in legitimate businesses, EUR 83 billion p.a. in lost sales in the legitimate economy for just 11 industry sectors and EUR 15 billion p.a. in Member State tax and social security revenue.

[5] Annex V: Selection of recent studies and tests on online platforms with a focus on illegal goods.

[6] The 2016 Global Consumer Shopping Habits Survey https://info.markmonitor.com/ccc_barometer

quarter of consumers have bought a product that turned out to be counterfeit, including fashion, footwear or electronics.

According to 94% of millennials (86% of those who are 35+), trust plays a role in making big purchases[7]. Of those consumers who were duped into buying illegal goods, 12% said they would not buy from that "brand" again, and over half expressed doubts[8]. These misleading practices and associated risks for consumers (e.g. lack of traceability, reduced control on quality).

2.3 Future-proofing: consumers are exposed to illegal goods across different types of platforms:

It is very likely that consumer behaviours and the market will change dramatically within the timeframe necessary to agree on a final text for the DSA proposals. Already today we see numerous consumer preferences and behaviours shifting, from traditional online stores to apps, social media, influencers and more. The new framework should factor this in and take a broad approach, covering all types of platforms, from those selling products to social media and search.

In the past consumers would actively search for a product online (through search engines or directly through a platform). Today the offers for products directly reach consumers through different channels and in particular via social media where goods (including illegal goods) are promoted. There is a real shift from proactive consumer behaviour, searching for products, to passive consumer behaviour, accepting the products and offers tailored to the consumer's browsing behaviour. Infringers are taking advantage of this shift to reach consumers easily and in great numbers.

2.4 Clarifying the need for platform action against illegal goods:

The experience of recent years shows that it is crucial to capture all illegal products within enforcement actions, as rogue traders are putting on the market substandard and dangerous goods for which nobody is responsible and for which the necessary safeguards are not in place. Building on the 2017 EU Commission Communication on Tacking Illegal Content Online[9] the DSA should clarify the responsibility of platforms to do more against illegal goods ensuring that the infringements captured by the DSA include both the infringement of EU level and national level rules. We therefore propose the following definition for illegal goods:

Illegal goods: *any product which infringes criminal and/or civil legislation, including intellectual property rights*

It is also important to ensure that the various types of illegal activities are captured in the legal framework. Some infringements will fall under criminal law at the national level and some under civil law (depending on the country).

The sale of illegal goods on platforms should not be mixed with freedom of speech issues. The aim of clarifying the legal framework around platform responsibilities in the case of illegal goods is to reduce the volume of illegal goods and protect consumers and businesses from harm.

2.5 Multiple roles of platforms:

[7] SurveyMonkey poll on brand trust in UK millennials, October 2018 (https://drive.google.com/file/d/1VikRY5l-YhmT5ZYputHJWfya7jk22ynt/view)
[8] Markmonitor, Global Online Shopping Survey 2018 – Facts, Figures, Fakery
[9] https://ec.europa.eu/digital-single-market/en/news/communication-tackling-illegal-content-online-towards-enhanced-responsibility-online-platforms

As technology evolves, it is important to ensure that all relevant platform roles should be captured under the DSA's scope reflecting the level of involvement of platforms in how the goods reach consumers. These roles include: providing an environment for the sale, purchase, advertising, payment, fulfilment or shipment of goods, or enabling third parties to do so.

2.6 Importance of having a clear set of legal obligations for action:

The removal of illegal goods is not a controversial subject. Often brands will flag illegal goods to platforms and provide the necessary elements for action. However, due to the lack of a clear framework platforms will often dispute the notices, react too slowly and not take sufficiently comprehensive and expeditious measures to address the infringements flagged (removing only one version of a notified product, removing one account not all the accounts, not blocking the use of a payments account or the actual user behind these accounts, etc.).

In addition, platforms will often refuse to implement actions against behaviours known to deceive consumers and facilitate the sale of illegal goods – such as the use of blurred logos, pictures with the trade mark elements concealed (presenting products only from certain angles) or photos or product identification details without authorisation from the right owners or the authorised retailers (in compliance with Commission Regulation (EU) No 330/2010 of 20 April 2010) – making it impossible for right owners and platforms themselves to determine the nature of the product sold to consumers.

In relation to illegal products, platforms will remove offers at the request of law enforcement authorities. However, the efficiency of platforms' stay down measures seems limited, all the more so when products are sold under brand names that can easily be altered ("pseudo-brands") and by sellers operating through a network of shell companies.

By allowing online offers to include blurred logos, pictures concealing trade marks, pictures presenting products only from certain angles or the use of photos or product identification details without authorisation from right owners, as well as pseudo-brand names, online platforms are in effect facilitating the sale of illegal goods. Such content deceives consumers and makes it impossible for right owners to determine the nature of the products offered for sale. In some instances, even where these behaviours are prohibited by online platforms' policies, they are not proactively enforced.

2.7 Illegal content must be effectively removed, and identities of sellers verified:

The number of rogue traders selling illegal goods is likely to keep growing if online platforms lack a clear policy on how to deal with repeat infringers. For example, some online platforms allow multiple infringements before a ban is imposed or take a lenient approach towards enforcing the ban - counting the number of infringements per brand and not per seller (banning sellers after three infringements, but counting the infringements per brand and not for the seller: a seller can accumulate multiple infringements under such approaches). Further, online platforms still do not have an effective model to ban repeat infringers, or indeed illegal content, once identified. If it is clear that a certain item should not be allowed, and the platform has recognised this fact by removing it, if nothing is done to prevent re-submission of that same item, the removal makes no material impact on the sale of illegal goods.

Moreover, the fact that platforms do not verify the identity of their sellers prevents the implementation of an effective policy against repeat infringers: further, certain professional sellers on platforms are empty shells and/or non-compliant with applicable legislation. This phenomenon is emphasised by new actors such as drop

shippers which act as opaque sellers' intermediaries for the sale of illegal goods on platforms and their delivery, notably via partnerships with the platforms and sellers.

2.8 A value chain approach where everyone needs to play their part:

All actors in the value chain should ensure that illegal goods are not offered to consumers. Once consumer trust is lost, all actors will be impacted. Brands, retailers, online platforms, advertisers, payment service providers and fulfilment and delivery service providers all depend on the others in the value chain to cooperate and act to prevent illegal goods from being offered to consumers in the first place.

Brands already contribute to this effort by monitoring platforms globally in order to take down illegal offers, conducting legal actions against infringers and cooperating with authorities such as customs involved in the fight against illegal goods and protection of consumers. However, these actions are mostly reactive and cannot be as effective as a stronger framework for preventive/proactive measures.

Online platforms, in their role as marketplaces, retailers, payment processors, fulfilment and customs clearing agents, delivery companies and more, are ideally positioned to prevent the sale of illegal goods online. The technology online platforms nowadays have and implement can clearly inform them of the multiple issues existing around specific illegal products, the rogue sellers behind the listings and sales and the details of complaints pertaining to them, thus allowing them to know the businesses that have been affected by the infringements and products concerned. They are the only link in the chain that knows both the seller and the consumer; no other party has such a wide visibility.

2.9 Public authorities and enforcement:

Authorities equally play a crucial role in the detection and removal of illegal goods. Customs authorities, police, market surveillance authorities and other law enforcement authorities are key in detecting and detaining infringing goods at the EU border and in the internal market. Improving their practical cooperation, both at an inter-institutional level and with private stakeholders, is essential if we are to maximise the targeted deployment of their scarce resources. In particular, it is crucial for public authorities to have access to the relevant (pre-arrival) data on the supply chain (seller, logistics, purchaser etc.) that only platforms can provide so as to enable enforcement and the prevention of illegal activities.

It would also be beneficial to provide an EU level framework for the fight against illegal goods sold across (inter alia) platforms, including an oversight body and the necessary common understanding of the issues (possibly common definitions).

3. Preventive and proactive measures are a crucial part of the solution

Voluntary action alone against illegal goods is clearly insufficient. There is an overall increase in the sale of illegal products across online marketplaces and platforms. Voluntary measures have not been implemented by all online players leaving important gaps.

Even in the case of those online players that have committed to implement voluntary measures there is very little transparency regarding what is removed, why and the actions taken in this area, making it very difficult

for brands to suggest ways to improve the efficiency of these measures. There are numerous examples[10], including during the current crisis, of measures that platforms are able to implement in order to detect and quickly remove illegal goods and content before their publication and to pursue their own enforcement actions.

Numerous best practices and technologies[11] are already employed by platforms that could be taken as a starting point for the update of the framework. To tackle rogue traders and illegal goods placed on the marketplaces, the future revision of the e-Commerce Directive should introduce relevant provisions to ensure that if online platforms implement any commercial technology for listings and marketing, this should also be used to detect and prevent fraud.

There are several relevant rulings, decisions and guidance documents that support making changes to the EU legal framework in this respect[12]. With the change of the digital landscape in the last twenty years and the new products and services that online platforms have gradually and unilaterally added to their universe, it would be difficult to find platforms, in Europe, for which the wording of the e-Commerce Directive is still appropriate, especially in terms of the liability exemption.

The e-Commerce Directive clarifies[13] that the provisions relating to liability do not preclude the development and effective operation of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology. The development and implementation of such technological solutions should be encouraged, for the benefit of online platforms, brands and consumers alike, and they should be an essential part of the online platforms' business model. Unfortunately, the logic of the limited liability regime creates disincentives for intermediaries to take proactive measures so they can continue not to be deemed responsible for the content they host.

At the international level, in the UN, UNCTAD[14] and the OECD[15] there have been strong calls in recent years towards a coordinated policy approach meant to boost consumer confidence in the new online tools such as online platforms and e-commerce more broadly.

The EU Commission pointed to the lack of a clear legal framework around the liability regime for intermediaries in the recent debates on the revision of the 2005 Unfair Commercial Practices Directive and before in the guidance for the Unfair Commercial Practices Directive. The role of the main consumer-facing platforms goes beyond merely hosting. They play a complex role and are extensively involved in the promotion, sale and

[10] https://ec.europa.eu/info/live-work-travel-eu/consumers/enforcement-consumer-protection/scams-related-covid-19_en#letters-sent-to-online-platforms

[11] Annex IV for examples of technologies that can be used for the fight against illegal goods on platforms.

[12] Annex II list of case-law, interpretations and guidance concerning the e-Commerce Directive and/or the role of platforms

[13] Directive 2000/31/EC Recital (40) Both existing and emerging disparities in Member States' legislation and case-law concerning liability of service providers acting as intermediaries prevent the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition; service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities; this Directive should constitute the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information; such mechanisms could be developed on the basis of voluntary agreements between all parties concerned and should be encouraged by Member States; it is in the interest of all parties involved in the provision of information society services to adopt and implement such procedures; the provisions of this Directive relating to liability should not preclude the development and effective operation, by the different interested parties, of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology within the limits laid down by Directives 95/46/EC and 97/66/EC.

[14] https://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=1724

[15] https://www.oecd.org/internet/consumer-protection-laws-need-updating-to-improve-trust-in-e-commerce.htm

delivery of goods to consumers. Claiming that they must avoid the implementation of proactive measures against illegal goods out of fear of becoming liable for the content is no longer a reasonable position to take.

3.1 Preventive and proactive measures: legislative action in the Digital Services Act

We propose the following updates to the current legal framework in order to address some of the most negative practices to which consumers and our members are often exposed:

Proposal	Clarification
Proactive/preventive screening obligation	The DSA should introduce an obligation for platforms to proactively screen for the sale and promotion of illegal goods - regardless of the platform, including search and social media - to prevent both the offering of illegal goods to consumers and to detect the distribution of illegal goods to consumers. In addition, platforms should clearly prohibit in their Terms and Conditions, and screen against, known fraudulent behaviours such as the use of blurred/cropped/concealed images, including the unauthorised use of brand images, and act more efficiently and more forcefully against repeat offenders.
Obligation to know and verify your sellers	The European framework of consumer protection relies on consumers being able to contact sellers, in order to be able to resolve problems. This should also apply online, and intermediaries (platforms and social media) should verify identities of sellers, and more generally the entire sales channel, before letting them sell their products to European consumers. Expanding Article 5 or 6 of the e-Commerce Directive could be one option. This should include simple due diligence checks akin to those in the Money Laundering Directive which could easily be employed by intermediaries of all sizes, for example ensuring that the contact data provided by sellers is verified (for business sellers: company address, VAT number, other registration numbers). There are numerous databases that can be checked[16], for example the EU Commission VIES (VAT database). There are also many third-party services providing identity verification. An additional seller identification source could be the customs registration required for third party sellers to sell into the EU[17]. Such measures would also enable platforms to react quickly and act on notifications regarding non-compliant sellers and no longer allow repeat infringers to regain access to the platform by simply creating a new account under a new virtual identity.

[16] Please see Annex III with examples of data that are already used today in various applications in order to verify different aspects around identify and compliance.

[17] https://ec.europa.eu/taxation_customs/business/customs-procedures/general-overview/economic-operators-registration-identification-number-eori_en#:~:text=EORI%20stands%20for%20%E2%80%9CEconomic%20Operators,exchanging%20information%20with%20Customs%20administrations.

	Policy makers should consider making platforms liable for the products in case the seller is not established in any form in the EU (or did not appoint a representative). The EU adopted a similar mechanism in Regulation (EU) 2019/1020 on Market Surveillance.
Notice and take down, transparency and cooperation/data sharing	The limited liability regime of hosting service providers should be maintained but strictly defined to apply only to actors providing pure hosting services. E-commerce platforms (i.e. platforms which allow for arranging the sale, purchase, advertisement, payment for or shipping of goods, or that enable a person other than an operator of such a platform to sell or offer to sell physical goods to consumers), should be clearly recognised as taking an active role in the transactions that they facilitate and required to comply with certain obligations, including the obligation to employ best efforts to prevent the posting of illegal content on their services. Third parties, including right owners, should continue to report illegal content to platforms but a clear harmonised framework for notice and take down procedures across the different platforms is also necessary. Platforms should be required to be fully transparent about the measures they take to fight against illegal content/products, including towards the brands. The new legal framework should enable, facilitate and overall define a framework for data sharing between platforms, law enforcement and right owners for the purposes of (1) detecting illicit goods, taking down online offers and shutting down supply chains in the physical world; and (2) efficiently sanctioning bad players. Such actions cannot be effective without the link to an obligation to verify user accounts (also with the view to preventing abusive accounts – e.g. fake consumer accounts, bot generated accounts). If it is shared cross-platforms it would permit authorities to fight efficiently repeat infringers which are operating on several platforms at the same time, often with the same contact details.
Remove products and inform consumers promptly	Under the current regime, once illegal products are identified, they should be removed by platforms. In the case of marketplaces, they know which consumers have already bought the product: indeed, they are the only part of the chain (besides the seller) to have this information. Platforms should have an obligation to inform consumers of the fact that the product they previously bought has since been removed from sale as illegal/counterfeit.

4. ANNEXES

4.1 ANNEX I: Recent legislation affecting platform obligations/role

Developments across many areas of policy in the past years point to the need for a recalibration in the role of intermediaries. Some of the most notable are:

- **New Deal for Consumers**: a clarification of the role of intermediaries and of the obligation to provide clear information to consumers regarding the contract and the applicable law. In addition, the final text allows Member States to impose further obligations on platforms.

- **The 2019 Platform to Business Regulation:** Article 3.5 requires platforms to provide information on the identity of the sellers (this obligation is similar to the one found in Article 5 of the e-Commerce Directive)

- **The 2019 Unfair Trading Practices Directive:** although only applying to B2B contracts in the sale of agri-food products (online or offline) the Directive includes a set of principles (cascading effect of unfair trading practices – and therefore the need to cover the entire chain) and a list of 16 unfair trading practices that could be referenced in the DSA.

- **The 2019 Market Surveillance Directive:** the obligation to appoint responsible contacts for the provision of compliance information, and the link this Directive creates with the role of fulfilment service providers that can establish legal responsibility.

- **The VAT framework** – marketplaces are liable to collect VAT for third country shipments as of 2021, therefore they will have to be aware of the identity of the traders.

- **The 2017 Commission Communication Tackling Illegal Content Online:** towards an enhanced responsibility of online platforms.

- **The 2018 Commission Recommendation on measures to effectively tackle illegal content online**

- **The 2019 Copyright Directive**

- **The 2018 Anti-Money Laundering Directive**

- **The 2016 General Data Protection Regulation:** provides for legal grounds for the processing of data in certain circumstances and with specific safeguards. However, often the GDPR is invoked by platforms as an obstacle that prevents them from sharing data regarding rogue traders with law enforcement agencies. This aspect could be clarified in the DSA: the GDPR does not apply to the data of legal persons and to commercial transactions.

- **To come: Update of Commission Regulation (EU) No 330/2010 of 20 April 2010 ("VBER"):** Implementation of European enforcement measures to fight against the illicit parallel market is contemplated in this updated framework. European national competition authorities have recently noted that the VBER and its guidelines may be affected by the Platform to Business (P2B) Regulation. European national competition authorities also acknowledge the increased importance of online platforms which have influenced and changed the behaviour of market participants and consumers, thus justifying an update of the VBER and its guidelines.

4.2 ANNEX II: Case law to be considered in the context of the Digital Services Act

The EU Court of Justice and national courts have clarified over the past years a number of elements around the role of intermediaries, essentially restricting the application of the exemptions for intermediary liability.

A selection of elements to consider in the current revision are explored in several decisions of the European Court of Justice:

- L'Oréal v. eBay (C-324/09) clarified that eBay is an "Internet Service Provider" (ISP) under the e-Commerce Directive, since it offers an online service that facilitates the relationship between seller and buyer. The Court also established that because of the way eBay operates, it could not be seen as a neutral or passive party to the transactions but on the contrary, its role is active and allows the platform to have both knowledge and control of the data related to the offers. Therefore, this ISP could not benefit from the "safe harbour" principle enshrined in the e-Commerce Directive.

- The European Court of Justice found in Eva Glawischnig-Piesczek v. Facebook Ireland Limited (C-18/18) that EU law does not preclude a hosting provider such as Facebook from being ordered by EU courts to remove identical and, in certain circumstances, equivalent comments previously declared to be illegal. As such, platforms may be required under EU law to proactively remove from their platform content that was previously declared illegal.

A growing tendency to recognise online intermediaries' responsibility can be also observed in the EU's national courts. For example:

- The Spanish Supreme Court confirmed through its ruling of 10 February 2011 (TS 72/2011) that an intermediary / service provider can be held liable if the illicit content hosted is notorious and does not depend on data or information that is not available to the intermediary.

- In January 2020, the Parisian Court held in Lafuma Mobilier / Alibaba et autres that Alibaba is a hosting provider and not merely an editor: https://www.legalis.net/actualite/alibaba-com-hebergeur-et-non-editeur/

- In Italy, in the case between Mediaset and Vimeo (693/19), Vimeo was not only requested to remove infringing content, but also prevented from posting new unauthorised content in the future. Due to the complex nature of its additional services to users, it was recognised as an active intermediary under the e-Commerce Directive.

- In another recent Italian decision (3512/19), a court in Rome condemned Facebook for hosting links leading to content infringing Mediaset's IP rights, despite receiving several injunctions for their removal.

- Other meaningful Italian rulings concerned Yahoo! (10893/11), the French hosting provider Dailymotion (342/18) and the American platform Break (8437/16), whose direct intervention in the uploaded content was considered sufficient to confirm their active role and effective knowledge about the infringing content. One of the leading editorial companies, Mondadori, also obtained an important victory against mere conduit service providers, including for future content that might be posted on "alias" links.

- The Federal Supreme Court in Germany ruled on 25 July 2019 (BGH-Urteil 25. Juli 2019 – I ZR 29/18) that an e-commerce platform such as Amazon may not use a brand for linked Google ads as part of a Google search that misleadingly displays not only the products of that brand but also third party products. Notably Ortlieb, the plaintiff, did not itself offer its products directly through Amazon, but

instead has a specific distribution system. This case may have a high impact on future Google ads on all online marketplaces.

- Confirmation that the Dutch courts are also moving towards a position that acknowledges online intermediaries' liability as to IP-infringing content can be seen in the Tommy Hilfiger v. Facebook 2018 case. Here a civil court in Amsterdam established the active role of the American social media platform in determining advertising content and its duty to prevent future violations with proactive action.

For a wider overview of case-law affecting online intermediaries, we refer you to the EUIPO's August 2019 case-law collection the liability and obligations of intermediary service providers in the EU, which provides an overview of developments and main conclusions of selected cases, including decisions of the CJEU and of national courts, issued between 2016 and the beginning of 2019

4.3 ANNEX III: Categories of data to be used for proactive & preventive measures

The below categories of information should be used by platforms to recognise patterns around illegal goods and establish tools to detect, prevent and/or remove future illegal goods listings.

User Identity
Attributes that are associated with the identity of a user
Examples: Name, email address, phone number, payment and account details

Behavioural Patterns
Preferences and patterns associated with the user
Examples: Browsing patterns, keyboard preferences, screen tilt

Locational Data
Location attributes associated with the user
Examples: fine and coarse location, GPS coordinates, shipping address, billing address

Device & Network Data
Properties of the device and network connection associated with the device
Examples: IP Information, Network ID, carrier network, device manufacturer & model

Transactional Data
Order details and order history associated with the user
Examples: order value, order velocity, transactions details and history of sales / reviews
Payment instruments:

- BIN (Bank details – name, country)
- Credit Card info (type of card, issuer, full number, expiry date, CVV and AVS codes)
- PayPal account information (account number, email used for identification)

Decisions
Business actions that can be used to screen out fraudulent or suspicious listings

Custom Data
Attributes that are unique to the business
Customs registration/identification numbers for third country operators
Example: Product details: name, size, colour, style number, quantity, price

Third-party Data
A variety of relevant third-party datasets
Example: Geo data, bank data, currency rates and conversions, social data

Time Series Data
As users interact with a website, every single step of that journey is collected and analysed to reveal insights into the users' traits.

Cross-User Data
Data points across multiple users can be utilised to see data patterns that reveal connections between users and logins.

Cross-organisational Data
Manually reviewed transactions across organisations get looped back into the system as soon as they are marked by analysts for fraud or other issues. This becomes a valuable data point that influences risk analysis across the network.

4.4 ANNEX IV: Available technologies/solutions for the fight against illegal goods

- Most of the data used by platforms is consolidated in databases. For example, platforms have access to structured global address databases to avoid delivery failures due to inaccurate address inputting. These databases should be used to prevent rogue sellers inserting false address information (e.g. using "Platform 9/2" instead of a real street name).

- In-house and third-party services allowing for the verification of the identity of private individuals and companies are also now widely available and are already used by some platforms but in a limited way.

- Artificial intelligence is already being used to identify linked accounts and prevent the same user from trying to register through different identities, spot previously suspended users trying to register again on the platform, etc.

- Anti-Fraud Systems, such as machine learning to detect fraud, already implemented by online platforms could be used to address illegal goods offered online[18].

- Image matching and image recognition software is widely used by platforms in order to steer sellers to the right level of quality and consistency. However, at the same time, our members note that platforms allow the use of blurred or partially cropped images that are used to disguise the sale of illegal goods by attracting consumers to what seem to be branded goods.

- Measures to address the use of bots for the creation of accounts, reviews, advertising or other interactions.

- As of 2021 platforms will be required to collect VAT for third country sellers. Any actor can already access the VIES database of the EU Commission or many other databases that provide company information. In connection with the payment details such a verification mechanism would provide traceability and ultimately liability.

[18] Please see Annex III for examples of data categories.

4.5 ANNEX V: Selection of recent studies/test purchases with a focus on illegal goods on platforms

- https://www.beuc.eu/publications/two-thirds-250-products-bought-online-marketplaces-fail-safety-tests-consumer-groups/html

- https://www.which.co.uk/news/2019/02/why-are-ebay-and-amazon-still-selling-killer-car-seats/

- https://www.which.co.uk/news/2020/03/online-marketplaces-coronavirus-update-ebay-and-amazon/

- https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

- https://www.electricalsafetyfirst.org.uk/blog/conline-the-hidden-dangers-behind-online-marketplaces/

- https://zvelo.com/unsafe-banned-and-counterfeit-products-on-the-rise-through-online-retailers/

- https://www.europol.europa.eu/sites/default/files/documents/catching_the_virus_cybercrime_disinformation_and_the_covid-19_pandemic_0.pdf

- https://ec.europa.eu/anti-fraud/media-corner/news/20-03-2020/olaf-launches-enquiry-fake-covid-19-related-products_en

4.6 ANNEX VI: Examples/experiences around notice and take down procedures for illegal goods

Notification procedures vary drastically from one platform to the next, ranging from a simple email to usage of propriety portals. This consumes considerable time for the right holders' teams responsible for processing them. For brands, the complexity of these counterfeit notification processes lies not only in the extremely lengthy and comprehensive information required by each platform to request the removal of a given product, but also in the absence of any consistent uniform procedures.

With the absence of a unified framework on how notifications must be conducted, each platform is free to implement a process of their choosing, with no obligation of consistency from one procedure to the next. While some platforms propose online forms to fill out directly on a portal provided via their website, others have not implemented this service and oblige any notification to be done via a printed form, rendering the notification process extremely arduous, and also request additional information such as brands' IPR certificates.

One platform, which opts for the printout requirement to declare any intellectual property infringement, requires a two-page form to be posted to the platform, along with the trade mark registration certificate in the name of the applicant and/or evidence regarding the ownership of copyright. The applicant is requested to select the reasons for the infringement from a list which includes trade mark and copyright infringement. Only one reason can to be selected per item. It is common for the platform to request further additional information, once the initial notice has been submitted, such as a letter of authority to act on behalf of the company or power of attorney.

For another platform, the procedure instead requires the brand to register in a database owned by the platform by completion of an online form and submission of applicable trade mark documentation. Once listed in the database, the procedure to notify a counterfeit product involves filling out an online form, in which it is required to list the infringements of the advertised product. Unlike the platform mentioned above, where only one infringement can be selected, in this case various infringements can be selected.

In some cases, an email is sent to confirm receipt of the infringement notification, although this is not systematic: with some platforms, no confirmation is ever sent, making it impossible to know when (or if) the request has been received and acknowledged.

On another platform, where varying models of one product are available for sale, a separate notification must be made for each variation of the same product (for example different designs or colours). It is not possible to select all variations of the listed product.

Removal time is also subject to significant variations. For some platforms, the removal of a product can take less than 24 hours, while others can take as long as 5 days.

Certain platforms share information about the seller with the notifying brand, others do not. The removal of the seller from the platform is mostly subject to case-by-case analysis, and platform processes again are not aligned.

The Digital Services Act: Towards a Healthy Online Platform Economy – Chapter 2

5. The Digital Services Act: the opportunity for a comprehensive solution

AIM represents over 2500 brand owners across the EU and beyond, covering a broad range of products[19]. Although the last few years have seen dramatic changes in all of our markets, the importance of brands to the European Union economy has not changed. Brands fuel product innovation, foster loyalty, trust and reputation with consumers, market and sell their products and services to meet consumer needs, and encourage and support competition on price and non-price metrics such as performance, quality and novelty.

Brands and consumers increasingly benefit from the digital economy. This makes a level playing field in the digital economy more than essential if brands are to continue to bring innovation and meet consumer needs. Competitive digital markets allow consumers to choose from whom they buy a product or service, challenge brands to compete and innovate, give brands opportunities to enter into new markets, and make them less dependent on a limited number of large companies.

Because of the role they play as an essential and unavoidable intermediary between an ever growing population of consumers and almost every brand, a small number of digital platforms that are referred to in the recent debates as gatekeeper or gatekeepers raise a number of challenges for the competitiveness of the digital economy as a whole. A vast number of brands, and other platform users, are in a dependency relation with such platforms. This is a relatively new development to this space which we consider requires an adequate legal framework and supervision of to protect the competitive digital economy ecosystem.

5.1 A healthy and competitive platform economy:

Increasingly, consumers are consulting only a handful of digital platforms, meaning online traffic and commerce is expected to continue consolidating. Today, nearly half of digital traffic is driven to ten digital platforms, and half of web sales are transacted through digital marketplaces.[20] Consolidation is predicted to continue to these platforms in the next five years, especially in light of the global COVID19 pandemic which has forced consumers online.

Defining the scope: The current debates seem to point to a need to adopt an ex-ante tool to address the negative effects resulting from some practices by the largest platforms. These online platforms act as "gatekeepers" or gatekeeper platforms in that they (1) hold a strategic position along the value chain between brands and their consumers and (2) are considered important, and virtually unavoidable, in many consumer facing markets (offering many types of products and services), having many suppliers depending on these channels and can therefore have the power to set the rules when it comes to market access or interaction with consumers. In today's economy, the use of such platforms is unavoidable for brands to reach their consumers, or for consumers to find certain products or services.

For example, imagine a brand not using the leading search engine to help consumers find information about its business. The future growth of brands in the digital economy depends on their ability to broadly communicate their vision, mission, brand value, product information, and to engage with consumers. Given traffic and commerce consolidation, brands will have to develop relationships with gatekeepers in new and innovative ways.

[19] For a detailed overview of the AIM National Associations and Corporate Members please visit the AIM website here https://www.aim.be/members/
[20] https://www.retaildive.com/news/forrester-half-of-online-sales-occur-on-marketplaces/504913/

Being at the centre: Far from being neutral digital sources of information and non-partisan fosterers of communities of interest, the gatekeeper platforms have evolved into complex entities providing a conglomeration of their own products (private label), services (cloud, payment, fulfilment, delivery), and content (advertising and more). The experience of past years shows that gatekeeper platforms also use the data of those who rely on their services to create competing products and services and place them in prominent positions above display of competitors.

The dynamics of online markets in which these platforms operate leads markets to "tip" in favour of such platforms, resulting in dominant market positions. This is because:

- the unique confluence of attributes that makes competition in gatekeeper platform markets different from more traditional markets: strong network effects, strong economies of scale, remarkable economies of scope from data, zero marginal costs, drastically lower distribution costs than brick and mortar firms, global reach, and consumer preferences for "one stop" or "one click" experiences; and
- Gatekeeper platforms can reduce potential competition by expanding into complementary / adjacent markets to maintain or even grow their market share.

Because of their position, gatekeeper platforms can have major effects on downstream markets and given their market share is durable, the effects can be long lasting. For example, if platforms "keep the gate closed" by imposing unreasonable conditions for use of their platform, it can be difficult or even impossible for brands to sell products at scale online. And if a platform provides insufficient access under reasonable conditions to brands, consumers are less likely to be able to find the brand's products. Thus, it is important that gatekeeper platforms engage in fair conduct, and do not act in a way that could undermine competition.

Competition authorities and scholars have identified certain conduct by "gatekeeper" platforms that has the tendency to distort competition[21]:

- Refusal to grant access to essential data or infrastructure
- Self-preferencing placement of the platforms' own products or services
- Entering adjacent markets by using data or information gained from their position
- Prohibiting data portability or multi-homing
- Prohibiting consumer choice on defaults for third-party options

In the EU, competition authorities, economists and lawmakers have started to focus on gatekeeper platform behaviour under the competition laws. In only the last year, attention and activity have increased around gatekeepers and the harm they pose to competition and consumers.

- In September 2019, 30 independent academics and policymakers published the "Stigler Committee Digital Platforms Report" describing the devastating effect from gatekeeper platforms anti-competitive practices on the economy and modern society.[22]
- In the last year, several Member States (Germany, France, UK, The Netherlands) have begun focusing on regulating gatekeeper platforms specifically, noting that competition law is considered insufficient to address attendant harms.

[21] An overview of the various national/international level initiatives to regulate platforms that act as gatekeepers or have an important gatekeeper effect/dependency effect on the multiple markets https://research.chicagobooth.edu/stigler/events/single-events/antitrust-competition-conference/world-reports-digital-markets

[22] Stigler Committee on Digital Platforms Final Report, 2019, at 48, 105-6 and Joaquin Almunia, Competition in the Online World, November 11, 2013.

- Reports and white papers submitted to the EU highlight the unique competition problems posed by gatekeeper platforms.[23]
- EU Competition Authorities have opened investigations into the practices of key gatekeeper platforms – echoing some of the national level enforcement cases.

5.2 Key suggestions for EU action in the DSA:

AIM calls on the EU Commission and Parliament to use the opportunity and address via the Digital Services Act the following aspects:

- Introduce a new concept of "gatekeeper" defined as companies that have both (1) "intermediary power" and (2) "paramount significance across several digital markets or sectors and markets"[24]. Such a definition would empower authorities to regulate those online platforms that are most likely to distort competition because of their positions in the market, while at the same time permit other online platforms which do not act as a gatekeeper to innovate and meet consumer demand.
- Companies that meet the criteria for gatekeeper platforms should be subject to new rules providing safeguards against the abuse of market power. Banning certain practices as such could have negative effects on the overall economy, limiting access to some essential services – however, some of the practices have been observed to have important anti-competitive effects, and therefore should be addressed. The services should not be confused with the practices; at this stage of development of the digital economy we believe it is possible to achieve to achieve innovation without unfair trading practice.
- Ensure a clear enforcement mechanism at the EU level ensuring coherence and legal certainty.

The new rules could permit gatekeeper platforms to engage in conduct which has the tendency to distort competition only where the platform could demonstrate that the conduct was on balance pro-competitive and the necessary additional pro-competitive compliance safeguards have been taken. For the following conduct, gatekeeper platforms would have the burden of proof of showing that it is pro-competitive:

- to refuse access to essential data or other infrastructure
- to self-preference placement of the gatekeeper's own products or services explicitly on the gatekeeper's platform
- to enter business users' markets by using data or information relating/belonging or generating by these users, gained from their position as a systemic platform, enabling platforms to launch a competing activity
- to prohibit data portability and multi-homing
- and to prohibit consumer choice on defaults for third-party options

[23] "Shaping Competition Policy in the Era of Digitisation," ERT, submitted December 31, 2018 (available at https://ec.europa.eu/competition/information/digitisation_2018/contributions/ert.pdf); and "Future-proofing of competition policy in regard to online platforms," Chief Economist for Netherlands Ministry of Economic Affairs and Climate Policy, submitted December 17, 2019 (available at https://www.government.nl/binaries/government/documents/letters/2019/05/23/future-proofing-of-competition-policy-in-regard-to-online-platforms/Brief+ENG.pdf); "Unlocking Digital Competition," UK Digital Competition Expert Panel, March 2019 (available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf).

[24] Similar to the Act on Digitalisation of German Competition Law published October 14, 2019.

About AIM

AIM is the European Brands Association representing brand manufacturers in Europe on key issues which affect their ability to design, distribute and market their brands.

AIM comprises 2500 businesses ranging from SMEs to multinationals, directly or indirectly through its corporate and national association members. Our members are united in their purpose to build strong, evocative brands, placing the consumer at the heart of everything they do.

AIM's mission is to create for brands an environment of fair and vigorous competition, fostering innovation and guaranteeing maximum value to consumers now and for generations to come. Building sustainable and trusted brands drives investment, creativity and innovation to meet and exceed consumer expectations. AIM's corporate members alone invested €14 billion in Research & Development in Europe in 2014, placing them fifth in the EU ranking of R&D investment.

AIM's corporate members

AB InBev • Arla Foods • Bacardi Limited • Barilla • Beiersdorf • Bel Group • BIC • Chanel • Coca-Cola • Colgate-Palmolive • Coty • Danone • Diageo • Dr. Oetker • Essity • Estée Lauder • Ferrero • FHCS/Vileda • FrieslandCampina • General Mills • GlaxoSmithKline • Heineken • Henkel • Jacobs Douwe Egberts • Johnson & Johnson • Kellogg • The Kraft Heinz Company • LEGO Group • Levi Strauss & Co. • Lindt & Sprüngli • L'Oréal • LVMH • Mars • McCain Foods • McCormick • Mondelez • Nestlé • Nike • Nomad Foods Europe • Orkla • PepsiCo • Pernod Ricard • Procter & Gamble • Puma • Reckitt Benckiser • Royal Philips • Sanofi • Savencia Fromage & Dairy • SC Johnson • Signify • Unilever

AIM's national association members

Austria Markenartikelverband • Belgilux BABM • Czech Republic CSZV • Finland FFDIF • France ILEC • Germany Markenverband • Greece EllhnikoV SundesmoV Biomhcaniwn Epwnumwn Proiontwn • Hungary Márkás Termékeket Gyártók Magyarországi Egyesülete • Ireland Food & Drink Federation • Italy Centromarca • MLDK • Netherlands FNLI • Norway DLF • Portugal Centromarca • Russia RusBrand • Spain Promarca • Slovakia SZZV • Sweden DLF • Switzerland Promarca • United Kingdom British Brands Group

EU Transparency register ID no.: 1074382679-01