International Trademark Association

14B rue de la Science, 1040 Brussels, Belgium
Tel: +32 2 880 3720 | Fax: +32 2 808 8464
inta.org

EU Digital Services Act package: open public consultation

INTA FULL COMMENTS – 8 September 2020

The present document reproduces some of the questions of the open public consultation on the EU Digital Services Act Package and the corresponding answers of the International Trademark Association (INTA), with further details and examples than the answers provided in the online form (de facto limited in characters).

QUESTIONS

1A. 10 - WHAT GOOD PRACTICES CAN YOU POINT TO IN HANDLING THE AVAILABILITY OF ILLEGAL GOODS ONLINE SINCE THE START OF THE COVID-19 OUTBREAK?

A worrying increased availability of illegal goods

With some borders closing due to coronavirus concerns and traditional illicit trade (drugs, firearms, etc.) being more difficult to smuggle, criminal organizations look to exploit consumers. For counterfeiters, the COVID-19 outbreak offered the "perfect" environment within which to operate. As the COVID-19 epidemic turned to a pandemic, consumers worldwide began to panic. There was no controlling this highly contagious virus, but there was one thing the general public could do: stock up. More goods have been available online – with people stuck in their homes. Counterfeiters follow these trends and will provide substandard goods to take advantage of these motivated buyers.

Criminals are taking their businesses online too. The Internet provides the ideal setting for counterfeiters to thrive in plain sight. Shoppers can order goods from a counterfeiter online and never know their identity. The counterfeiter can accept credit card transactions from across the globe anonymously and ship the goods directly to the consumer.

On March 23, the Organisation for Economic Co-operation and Development and the European Union Intellectual Property Office released a report on counterfeit medicines stating: "[i]n 2016, international trade in counterfeit pharmaceuticals reached USD 4.4 billion, threatening public health and safety, while enriching criminals and organised crime." The report goes on to estimate that up to 169,000 children treated with counterfeit drugs succumb to pneumonia every year and counterfeit anti-malarial medication has led to up to 116,000 deaths. Clearly with counterfeits, there are no guarantees that consumers are getting the results they are seeking when buying these goods.

The week of March 3, 2020, INTERPOL conducted Operation Pangea XII, which coordinates the law enforcement efforts of 90 countries worldwide targeting counterfeit medicines and medical products. The Operation resulted in 2,000 sites selling products related to coronavirus, with 30 % selling counterfeit surgical masks. The Operation resulted in the seizure of 34,000 counterfeit and

substandard goods related to COVID-19. INTERPOL's Secretary General Jürgen Stock stressed that "Once again, Operation Pangea shows that criminals will stop at nothing to make a profit. The illicit trade in such counterfeit medical items during a public health crisis shows their total disregard for people's wellbeing, or their lives."

The goods seized in this one week amounted to € 12.5 million and lead to 121 arrests. The mean profit for each criminal was about €100,000 for one weeks' worth of trafficking counterfeit goods. It is certainly a high-reward crime.

Catherine De Bolle, Executive Director of Europol also warned "*Criminals abuse fears around the pandemic by selling medicines online which claim to cure the coronavirus. Not only are these medicines fake, but dangerous too. Don't buy them*!" Europol released a report on how criminals are exploiting the COVID-19 Crisis on March 27.

Good practices

The private and public sectors must work together to combat this counterfeiting activity in order to protect consumers at a time when they are most vulnerable. A strong public-private collaboration is a valuable start to prevent this criminal activity.

Anticounterfeiting collaboration means looking at successes around the world and replicating them or using them as launching pads for similar efforts. Many countries have excellent IP crime enforcement agencies, such as the City of London's Police Intellectual Property Crime Unit. Established in 2013, it has the responsibility to investigate and deter serious and organized IP crimes in the UK and to protect consumers from harm, focusing on IP crimes that have public safety implications. Since its inception, it has investigated IP crimes worth more than £100 million concerning counterfeit goods or digital piracy, and suspended more than 30,000 websites selling counterfeit goods.

Another model worthy of duplication is the US IPR center—the National Intellectual Property Rights Coordination Center, which brings together 23 partner agencies, consisting of 19 key federal agencies, Interpol, Europol, and the governments of Canada and Mexico in a task force setting. The task force structure enables the IPR Center to effectively leverage the resources, skills, and authorities of each partner and provide a comprehensive response to IP theft. INTA recently published a paper to help create and promote such IPR centers in other jurisdictions and countries.

The success of this model is quite evident in the recent actions of the US IPR Center. As the COVID-19 pandemic let to a rise of counterfeit medicines and PPE equipment, the Center spearheaded the US Response with the April 15 launch of "Operation Stolen Promise" to combat COVID-19 related fraud and criminal activity. As of July 14, Homeland Security Investigations reported the seizure of almost $6.9 million in illicit proceeds and the seizure over 969 shipments of mislabeled, fraudulent, unauthorized or prohibited COVID-19 test kits, treatment kits, homeopathic remedies, purported anti-viral products and personal protective equipment (PPE) in coordination with US Customs and Border Protection. Additionally, the US government has investigated 554,374 COVID-19 related domain names. While the number of investigations is impressive, the private sector is lacking information on outcomes and consequences to perpetrators. As addressed in 2A.18 & 19, it is important that brand owners have access to this information whether from platforms or governments.

INTA also applauds the Commission for the European Anti-Fraud Office (OLAF) enquiry into counterfeit COVID-19–related products. Since March 19, OLAF has been collecting intelligence and

information on the issue. OLAF and national customs administrations are working together to prevent counterfeit goods from entering the European Union. INTA has supported some of the Commission's outreach to the private sector to help these efforts.

INTA supports the development of a model at both the national and EU level where the private sector and public sector work together to stop illegal activity on legitimate channels for goods, especially when consumer have to rely so heavily on the Internet during quarantine. The public and private sectors, including the intermediary services providers and trademark owners, all have an interest in protecting consumers from illegal activity.

Finally, the Registrar Stakeholder Group at ICANN has put together a document that outlines and describes potential approaches to addressing illegal behavior under the circumstances of the current COVID19 pandemic. These approaches include measures to identify and take down domain names that seek to spread false information about the virus and potential cures and which also seek to sell and distribute counterfeit PPE and other medical products. See https://rrsg.org/wp-content/uploads/2020/03/Registrar-approaches-to-the-COVID-19-Crisis.pdf

1A.20 - WHAT ACTIONS DO ONLINE PLATFORMS TAKE TO MINIMIZE RISKS FOR CONSUMERS TO BE EXPOSED TO SCAMS AND OTHER UNFAIR PRACTICES (E.G. MISLEADING ADVERTISING, EXHORTATION TO PURCHASE MADE TO CHILDREN)?

INTA supports best practices for search engine advertisements in Addressing the Sale of Counterfeits on the Internet. The publication is a roadmap for voluntary collaboration between all of the parties involved in fighting counterfeiting provides recommendations for search websites, online marketplaces, payment service providers, and trademark owners, as well as of social media, logistics, registrars and registry companies. This document is currently under revision and the final, updated version will be provided to the Commission upon completion.

The best practices highlighted in the above referenced document are measures that reputable online platforms are taking in order to minimize risks to consumers. Focusing on online trading platforms, these recommendations include:

- Online trading platforms should strengthen and streamline procedures for identifying and taking more effective action against repeat offenders, as well as tighten repeat offender policies.
- Online trading platforms should employ preventive measures to reduce the sale of counterfeits by anonymous counterfeiters, such as filters and identity verifications and improved customer screening.
- Subject to applicable privacy laws, online trading platforms should improve disclosure policies to facilitate access by trademark owners and law enforcement authorities to information about counterfeiters, including seller identities and sales information.
- Online trading platforms should add search and enforcement application program interfaces (APIs) that allow trademark owners to conduct automatic scanning and retrieval of listings and seller information, thereby greatly improving the efficiency of monitoring and review efforts.
- Online trading platforms should implement commercially reasonable, automated "know your customer" measures to verify the identities and addresses of sellers and make sure they are not operating under multiple false accounts.

- Online trading platforms should operate an effective notice and takedown program with internal mechanisms to make sure the listings for counterfeits do not come right back up or the counterfeiters find some other way to game the system.
- Online trading platforms should accept removals based on a wider range of IP rights, including copyrights and design rights, which have become necessary as counterfeiters shift away from using discernible trademarks in their listings in order to avoid takedown.
- Online trading platforms should interface on a regular basis with trademark owners upon request to learn about infringements to a particular trademark and how counterfeiters are getting around current restrictions.

The EU has existing commercial models where consumers may confidently purchase goods online with government oversight. A good example is online pharmacies.

Certain well-known, online platforms have developed other best practices, policies and processes to address counterfeit sales. Notably, some platforms have embraced new technologies (e.g. blockchain, artificial intelligence, machine learning, etc.) to help combat counterfeits sales and distribution. For example, one social media company has published a Counterfeiting Guide that contains its current terms, policies, and enforcement procedures on its platforms. Other well-known e-commerce sites have streamlined processes for removing counterfeits and use AI and other advanced machine learning to scan their marketplaces for infringing products and counterfeit goods. Blockchain companies help track and trace genuine goods through various supply chains including online distribution. Search engines also use sophisticated machine learning-based systems developed by their engineering teams to try to prevent ads for counterfeit products. A well-known, social media platform applies machine learning and artificial intelligence technologies to help block or reduce the distribution of potentially counterfeit content, and to review both its marketplace posts and ads against its policies before they go live. As the Commission will note, adoption of new and innovative means to identify and reduce the distribution of counterfeit goods is ongoing and should be further encouraged.

While some platforms have taken helpful steps to address harms such as those detailed above, there are other platforms which are less diligent, or in some instances encourage activity which results in consumers being exposed to scams, unfair practices and sales of counterfeit products. These online platforms seek to attract users through provision of access to infringing content or goods, which is often accompanied by advertising that is fraudulent in nature, and/or exposes users to malware or do not employ measures to protect minors from gambling or pornographic advertising.

1D.11 - DO YOU USE WHOIS INFORMATION ABOUT THE REGISTRATION OF DOMAIN NAMES AND RELATED INFORMATION? PLEASE SPECIFY FOR WHAT SPECIFIC PURPOSE AND IF THE INFORMATION AVAILABLE TO YOU SUFFICIENT, IN YOUR OPINION?

Yes.

Brand owners use and rely upon WHOIS information to try to identify the ownership of domain names that infringe their trademarks. When brand owners detect a domain name that is registered to a third party and which contains an exact match or close typographical variation of the brand, they need to know who registered the domain name to determine whether it is infringing or likely to infringe their rights (i.e. “for the establishment, exercise or defense of legal claims” Art. 21 of the EU

General Data Protection Regulation, "GDPR"). If a domain name is determined to be infringing, WHOIS information is used to establish proper jurisdiction and venue to bring a claim, what jurisdiction's law applies, and for other litigation-related purposes. For example, in the US the Anticybersquatting Consumer Protection Act (ACPA), requires, "sending a notice of the alleged violation and intent to proceed under this paragraph to the registrant of the domain name at the postal and e-mail address provided by the registrant to the registrar." United States Code,15 U.S.C. § 1125(d)(2)(A)(ii)(II)(aa).

Brand owners also use WHOIS information to help decide whether a link or website is trustworthy (i.e. whether an email sender or website host is who they say they are), and to know how to contact the domain name owner if there is a technical problem with the domain name.

Since being redacted in efforts to comply with the requirements of the GDPR, the information now available in the public WHOIS system is no longer sufficient for these purposes, and ICANN-contracted parties are most often not providing the redacted data upon request. This is more fact than opinion. See: https://clarivate.com/markmonitor/blog/gdpr-whois-and-impacts-to-brand-protection-nine-months-later/

The implementation of GDPR has resulted in ICANN changing its longstanding contractual requirement to make public all collected domain name registration data. As a result, it has become much more difficult, if not impossible, for brand owners to identify who is behind websites that advertise or sell counterfeit goods. ICANN's changes to its open WHOIS policy were implemented through a Temporary Specification effective May 25, 2018. The Temporary Specification requires Registrars and Registries to provide reasonable access for legitimate purposes such as to conduct investigations of cybercrime, DNS abuse and intellectual property protection. However, in practice, registrars and registries often do not respond to even clear-cut requests for registrant information in a timely manner if they respond at all.

Moreover, because counterfeit goods can, at times, pose risk to the public health and safety of consumers, it is also important for registrars and registries to promptly investigate reports of abuse involving domain names that they sponsor. The EU should support the Intellectual Property community's continued advocacy efforts to push for a standardized system for reasonable and balanced access to nonpublic registrant data and provide the necessary interpretative guidance to encourage third parties to cooperate with law enforcement and intellectual property owners The lack of clarity in the application of GDPR has created an untenable situation in terms of ensuring quick access to reliable and accurate contact information for domain name registrations. INTA members have been at the forefront of the ongoing engagement with ICANN to resolve this issue to the benefit of rights holders and consumers.

2A.3 -- WHAT INFORMATION WOULD BE, IN YOUR VIEW, NECESSARY AND SUFFICIENT FOR USERS AND THIRD PARTIES TO SEND TO AN ONLINE PLATFORM IN ORDER TO NOTIFY AN ILLEGAL ACTIVITY (SALES OF ILLEGAL GOODS, OFFERING OF SERVICES OR SHARING ILLEGAL CONTENT) CONDUCTED BY A USER OF THE SERVICE?

- ☑ Precise reason why the activity is considered illegal
- V Precise location: E.g. URL
- ☑ Description of the activity
- ☑ Identity of the person or organisation sending the notification. Please explain under what conditions such information is necessary:
- ☑ Other, please specify

INTA answers are limited to information that brand owners need to provide.

INTA recommends best practices for search engine advertisements in Addressing the Sale of Counterfeits on the Internet. As mentioned previously, this publication is a roadmap for voluntary collaboration between all of the parties involved in fighting counterfeiting online. The document is currently under revision and the final, updated version will be provided to the Commission upon completion.

As a best practice, trademark owners should provide to online platforms and other intermediaries, at their request, a list of keywords commonly used by sellers for the purpose of offering for sale counterfeits, to assist such platforms and other intermediaries with their voluntary measures for combatting counterfeiting online.

Before submitting a notice, trademark owners should take measures that are reasonable under the circumstances to verify that the material is not authorized by the trademark owner and preserve dated website documentation of such unauthorized material.

In working with platforms and other intermediaries on combating online sales of counterfeits, trademark owners should provide information such as the following:

- Identification of the material alleged to be illegal;
- Information identifying where the alleged illegal material is located;
- Proof of ownership of a relevant trademark or other IP right, as applicable, in one or more applicable jurisdictions; and
- A statement made under penalty of perjury that the notifier is the trademark owner or is authorized to act on the trademark owner's behalf and a good faith belief that the use of the material in the manner complained of is not authorized by the trademark owner.

IP rights holders should be able to show proof of their rights in registered marks or copyrights as well as specific details around why the goods or content is illegal (e.g., packaging, design, etc.). While a test purchase that has been verified as "illegal" is certainly sufficient, requiring test purchasing is unduly burdensome and unnecessary in many, if not most, situations. From a general user perspective, any evidence including, but not limited to, that present in chats, conversations, sales negotiations, etc. from the provider that indicate the activity is illegal should be sufficient.

2A.6 - WHERE AUTOMATED TOOLS ARE USED FOR DETECTION OF ILLEGAL CONTENT, GOODS OR SERVICES, WHAT OPPORTUNITIES AND RISKS DOES THEIR USE REPRESENT AS REGARDS DIFFERENT TYPES OF ILLEGAL ACTIVITIES AND THE PARTICULARITIES OF THE DIFFERENT TYPES OF TOOLS?

Automated tools have been employed by platforms for several years to effectively scan for and detect suspected counterfeit goods. The risks of employing such tools include over or under-detection. Measures can be employed to allow for access to be restored in the event that goods are wrongly identified as infringing. Issues to consider include the following:

- Using automation to detect *illegality* is can be difficult. Automated tools are not well suited to understand the nuance of local law, nor the context that is so frequently required to determine if something is unlawful (e.g., what constitutes hate speech vs. self-identification, what's true/false for defamation analysis, what's authorized or genuine vs. counterfeit) – much of this will always be in the expertise or knowledge of the aggrieved party. Automated tools can be helpful in searching the suspected counterfeits but may need a human review to improve accuracy.
- Local laws also vary considerably from Member State to Member State – what might be unlawful in one place may be legitimate free expression in another. Automation is not able to parse out this nuance.
- Automation can be used to enforce a platform's policies, which in many cases, can overlap with (but are not intended to be coexistent with) local law.
- As many advances have been made recently, it's impossible for automation to detect bad content with perfection – as a technical matter, small differences can mean systems do not identify it, and adversarial bad actors who are motivated to abuse policies and evade enforcement are sophisticated in their approach.
- Greater reliance solely on automation poses the risk of over-blocking and erroneous removal of legal content, which would have a chilling effect on speech and other fundamental rights.
- Automation should remain a voluntary best practice with platforms having the flexibility to choose solutions that work best for their size and business model.

2A.7 - HOW SHOULD THE SPREAD OF ILLEGAL GOODS, SERVICES OR CONTENT ACROSS MULTIPLE PLATFORMS AND SERVICES BE ADDRESSED?

WHOIS has been one of the most useful tools in identifying connections that enables addressing illicit activity across a variety of platforms, which is now unavailable as a result of the failure by registrars and registries to permit access to data in order to conduct such searches, which has been underwritten by policies at ICANN. One of the adverse consequences of the inability to obtain WHOIS information, and conduct "reverse WHOIS searches" is the difficulty in connecting different bad actors across platforms and services. The current ICANN policies do not adequately take into account the legitimacy of interests that would be served by allowing access to WHOIS data for these purposes.

Therefore, as a result of lack of access to WHOIS, it is at the outset quite difficult (and sometimes not possible) to have visibility into the linkages between illegal activity across different platforms. Rights owners must be able to contact the correct platform. It is essential, therefore, that WHOIS data be made available to avoid a situation where the rights owner contacts an intermediary that may not be directly responsible for the content at issue. It is important that this critical issued be addressed and clarified by the EU in order to permit such activity towards addressing systemic harms.

INTA supports a trusted seller program as something to consider in the E-Commerce Directive. There is similar precedent in the EU Through EU Regulation 699/2014 issued on 24 June 2014, the

European Commission created and established a common logo to be shown for pharmacies selling pharmaceutical products online to guarantee consumers that the goods they were offering are fully legal, and that the owner of the website is an actual pharmacy (registered and licensed by a Member State). This regulation set a number of technical requirements and specifications to warrant a high level of security and avoidance of any fraudulent use of said logo. Thus, any and all pharmacies legally offering their products online must clearly include this logo in all the pages of its website. By clicking on this logo, consumers are led to the official website of the corresponding member State Agency confirming that said pharmacy is legally registered and licensed, therefore confirming to consumers that they may trust that particular website. The display of this logo instills consumer confidence of online purchases. Perhaps the Commission could explore a similar way to recognize trusted sellers of all types through the upcoming Digital Services Act.

In 2017, Global Financial Integrity estimated the annual value of global drug trafficking between €380 billion and €580 billion, making it the second most lucrative illicit market measured after that of counterfeit and pirated goods (valued at €1.37 trillion in 2013). Most counterfeit sales occur on the Internet where anonymous sellers may post photos of genuine goods on trusted platforms to dupe unsuspecting consumers into buying their goods. This "bait and switch" is an especially vexing problem because the goods cannot be inspected before sale. The consumer relies on a photograph. The creation of an administrative body to validate the trustworthiness of a vendor might be considered in trying to solve this issue. If an administrative agency is created across the EU, it might be helpful in harmonizing practices. The agency could have some limited powers to quickly adjudicate disputes between online sellers (both platforms and vendors) and rights holders in instances where it appears counterfeit goods are being substituted for authentic goods.

Another possibility if for the creation of an EU -wide administrative agency to efficiently handle disputes under the revised Digital Services Act. Enforcing against counterfeiting on the Internet is an arduous task as anonymous sellers can post and remove content in a matter of minutes. If there is an efficient way to get information from selling platforms or make quick determinations about counterfeiters, swift action could lead to better results against online counterfeiters. Any administrative decisions could be appealed to the court system. A government body looking at enforcement on a case by case basis would help to make determinations without a "one size fits all" approach. Keeping these proceedings efficient and low cost would allow rights holders of all sizes to enforce their rights. It might also minimize the need for private agreements between larger brand owners and the platforms thus leveling the playing field for all rights holders.

An example of a similar practice focused on piracy in Spain. Established in 2012, the Antipiracy Commission (AC) is an administrative body under the Ministry of Culture and Sport with the primary function to safeguard copyrights in the digital environment. This body is composed by public officers and, therefore, not a judicial body. The AC has been enacted in the Intellectual Property Act and later on Royal Decrees that develop the legislative order. Under Spanish law, the intellectual property is limited to copyrights, while industrial property covers trademarks, patents and designs.

There is a simple process for piracy complaints to the AC online through the Ministry Portal. The owner of copyright or its representative must provide evidence of the attempt to settle amicably. An attempt to send a cease and desist letter with identification of the copyright, its owner, and e- location of the infringement is sufficient. This prior notice requirement is not necessary in cases where the Internet Service Provider (ISP) does not offer a valid e-mail address, given the impossibility of serving the notification. If the copyright owner has difficulties on finding the identity of the infringer,

the AC will issue a petition to an Administrative Court (a judicial body) for the Judge to issue an order directed to online intermediaries to compel them to provide this information.

Once the complaint is accepted, the AC will elaborate a proposal of resolution that will be sent to the infringer with the request of either i) voluntary remove the illegal content with 48 hours or ii) contest the petition. In 2018, around 39 % of infringers voluntarily removed content once they received this first notification without the need of the copyright owner to pursue the case further. However, the owner of the copyright is not precluded from using any other civil/criminal or administrative actions available that it might deem necessary if they file a complaint and receive remedies through administrative action with the AC.

If the suspected infringer contests the copyright owner's compliant in 48 hours, the AC will issue a decision. If the content is found to be an act of piracy, the result is a binding administrative decision against the infringer. The decision can order not only the removal of the illegal content, but also shut down the webpage, the publication of the decision and/or the cancellation of the domain name. If the infringers refuse to comply with this administrative final order, the AC will refer this refusal to the Judicial Body for judicial execution of the decision. If a decision is rendered declaring the infringement of IPRs, the ISPs must comply with the decision and block the site within 24 hours. In default of voluntary compliance, the AC can also order the internet service intermediaries, payment providers and advertising services providers to suspend the service they are providing to the infringer. If the infringer repeats the illegal activity, the AC can impose fines going from €150,000 to €600,000.

The Spanish Civil Courts have also rendered decisions with similar "effective consequences". For instance, the very recent judgment rendered by the Commercial Court no. 7 of Madrid on 11 February 2020 requesting blocking orders against ISPs in relation to pirate websites through which football games could be watched, including an order to weekly block within three hours access to any pirate websites identified by the Plaintiff (Telefónica Audiovisual Digital) until 25 May 2022. However, it should be noted that in said case the ISPs had accepted the claim (so the Commercial Court only had to make sure that the order to be issued did not amount to a fraud or was not against public interest).

On July 20, the AC reported in the last year it received 671 complaints, of which 94% were found to have illegal content resulting in the removal of more than 640,000 instances of illegal content from the Internet. INTA urges the Commission to consider an agency with a similar process to be as effective against counterfeiting.

2A. 8 - WHAT WOULD BE APPROPRIATE AND PROPORTIONATE MEASURES THAT DIGITAL SERVICES ACTING AS ONLINE INTERMEDIARIES, OTHER THAN ONLINE PLATFORMS, SHOULD TAKE – E.G. OTHER TYPES OF HOSTING SERVICES, SUCH AS WEB HOSTS, OR SERVICES DEEPER IN THE INTERNET STACK, LIKE CLOUD INFRASTRUCTURE SERVICES, CONTENT DISTRIBUTION SERVICES, DNS SERVICES, ETC.?

Online marketplaces have different business models and user profiles, so it is difficult to formulate a "one size fits all" regulation or enforcement standards across all online intermediaries. However, acknowledging the different models, online intermediaries should use commercially reasonable efforts to fight counterfeiting as may be applicable to their respective business models. Some methods for doing so could include:

- proactively scan listings and remove high confidence counterfeits;
- create a list of repeat counterfeit sellers for platforms to maintain in cases of multiple violations by a single seller;
- provide tools that allow verified trademark owners with a history of good faith takedowns to report counterfeit listings for takedown, e.g., platforms may employ appropriate policies and procedures to deter the use of these tools to limit lawful secondary sales or other abuse;
- perform serialization validity checks for serialized products; and
- prohibit the sale of counterfeit or unlawful products, include a requirement to verify the identity of their business customers and require sellers to maintain and disclose identity/location/source/authenticity records to the platform upon request.

2A. 19 - WHAT TYPE OF INFORMATION SHOULD BE SHARED WITH USERS AND/OR COMPETENT AUTHORITIES AND OTHER THIRD PARTIES SUCH AS TRUSTED RESEARCHERS WITH REGARD TO THE USE OF AUTOMATED SYSTEMS USED BY ONLINE PLATFORMS TO DETECT, REMOVE AND/OR BLOCK ILLEGAL CONTENT, GOODS, OR USER ACCOUNTS?

While private sector partnerships with law enforcement authorities has resulted in the successful removal of infringing websites and counterfeit goods, more data and information from law enforcement activities would be helpful in further strengthening these efforts. For example, in many of the operations, brand owners and brand protection companies are not given any data on the number of websites shutdown, domain names suspended or deleted, or pirated content removed. Because this important data is not shared with private sector partners, it is difficult to know the effectiveness and impact of these. If law enforcement authorities would share more details and data related to the success of their operations, more cooperation and collaboration could be fostered. INTA urges law enforcement authorities to contribute more data and information to its private sector partners in order to strengthen these partnerships and make an even greater impact.

INTA wishes to draw the EU Commission's attention to the resources and talents of academic institutions and scholars who are doing research into the future of intellectual property protection. One excellent example is the European Observatory on Infringements of Intellectual Property Rights, which produced some of the reports mentioned in the answer to question 1A.10. Another example is Michigan State University's Center for Anti-Counterfeiting and Product Protection (A-CAPP). This research and scholastic program provide valuable research data and information that can help shape the brand protection strategies around the world.

2A. 21 - IN YOUR VIEW, IS THERE A NEED FOR ENHANCED DATA SHARING BETWEEN ONLINE PLATFORMS AND AUTHORITIES, WITHIN THE BOUNDARIES SET BY THE GENERAL DATA PROTECTION REGULATION?

Please select the appropriate situations, in your view:

☑ For supervisory purposes concerning professional users of the platform - e.g. in the context of platform intermediated services such as accommodation or ride-hailing services, for the purpose of labour inspection, for the purpose of collecting tax or social security contributions

- ☑ For supervisory purposes of the platforms' own obligations – e.g. with regard to content moderation obligations, transparency requirements, actions taken in electoral contexts and against inauthentic behaviour and foreign interference
- ☑ Specific request of law enforcement authority or the judiciary
- ☑ On a voluntary and/or contractual basis in the public interest or for other purposes

INTA believes intra- or cross-industry collaboration is essential to making progress on the battle against counterfeit goods. Every industry sector that touches the counterfeit ecosystem, needs to coordinate their efforts. This includes domain name registrars and registries, search, payment processors, marketplaces, and package shippers. One brilliant example of such coordination can be found in the work of the Center for Safe Internet Pharmacies (CSIP). This non-for-profit organization, comprised of representatives from all of the industries identified above, came together in 2011 to address the growing problem of harmful illegitimate pharmacies. Through CSIPs' efforts, tens of thousands of rogue pharmacies have been suspended or had their operations thwarted as a result of coordinated efforts by each of these industry sectors.

While some marketplaces and social media platforms have improved their collaboration with brand owners and are demonstrating more commitment to counterfeit detection and enforcements, some have done little to share data, information, and best practices with each other to aid in combatting the counterfeit problem. Whatever the reason -- fierce competition or data privacy considerations, social media platforms should try and overcome these barriers and work on common solutions that can be adopted by the e-commerce and social media industries. Imagine the efficiencies gained if a counterfeit seller, removed on one marketplace, could be removed on another marketplace simply through the use of a trusted communication from one marketplace to another. If counterfeiters knew that a takedown in one marketplace would mean removal from others, more may be deterred from establishing counterfeit sites on multiple platforms.

II. 2 - THE LIABILITY REGIME FOR ONLINE INTERMEDIARIES IS PRIMARILY ESTABLISHED IN THE ECOMMERCE DIRECTIVE, WHICH DISTINGUISHES BETWEEN DIFFERENT TYPES OF SERVICES: SO CALLED 'MERE CONDUITS', 'CACHING SERVICES', AND 'HOSTING SERVICES'. IN YOUR UNDERSTANDING, ARE THESE CATEGORIES SUFFICIENTLY CLEAR AND COMPLETE FOR CHARACTERIZING AND REGULATING TODAY'S DIGITAL INTERMEDIARY SERVICES? PLEASE EXPLAIN.

The E-Commerce Directive provides a sufficiently flexible means of classifying the activities of intermediaries, with specific focus on the types of activities which are passive in nature – such as acting as mere conduits, caching and hosting. These distinctions remain relevant today.

II.3 - FOR HOSTING SERVICES, THE LIABILITY EXEMPTION FOR THIRD PARTIES' CONTENT OR ACTIVITIES IS CONDITIONED BY A KNOWLEDGE STANDARD (I.E. WHEN THEY GET 'ACTUAL KNOWLEDGE' OF THE ILLEGAL ACTIVITIES, THEY MUST 'ACT EXPEDITIOUSLY' TO REMOVE IT, OTHERWISE THEY COULD BE FOUND LIABLE). ARE THERE ELEMENTS THAT REQUIRE FURTHER LEGAL CLARIFICATION?

The Digital Services Act should be written in a manner that discourages conscious negligence. “Expeditiously” could be better defined and might include a 48-hour period for response.

II.4 - DOES THE CURRENT LEGAL FRAMEWORK DIS-INCENTIVIZE SERVICE PROVIDERS TO TAKE PROACTIVE MEASURES AGAINST ILLEGAL ACTIVITIES? IF YES, PLEASE PROVIDE YOUR VIEW ON HOW DISINCENTIVES COULD BE CORRECTED.

INTA believes that encouraging services providers to take proactive measures where commercially feasible is a good framework and does not disincentivize actions. It is in the interests of service providers to be proactive in order to ensure a safe and beneficial experience for the consumer. However, the burden to ensure legality should not necessarily be placed entirely on third parties. For anticounterfeiting efforts, it is up to trademark owners to enforce their rights. The rights owner relies on information on counterfeiters in order to further investigate counterfeit activities and bring civil actions against these criminals. In many cases, when trademark owners try to work with intermediary service providers to obtain information on sellers that are suspected of selling counterfeits on these platforms, the rights owner is denied information on those sellers due to privacy concerns for the sellers. The current data protection regime in the EU would expose the intermediary service providers to violations of the General Data Protection Regulation and thus the identities of counterfeiters are kept from rights holders.

Under the current structure, trademark owners are forced to go through law enforcement or pursue legal action in order to obtain the identity of these counterfeiters. The vast amount of counterfeiting on the Internet does not make it practical for rights owners to proceed with these sorts of excessive measures to investigate every counterfeit listing. Therefore, INTA supports some means be established to allow intermediary service providers to share information with rights holders in a way that does not interfere with any privacy laws, and provides balance in determining the best outcomes for the end user. An unintended consequence of overly restrictive approaches to enforcing privacy rights is that the very consumer that privacy laws are engineered to protect may also be the same consumer who is injured by a counterfeit product.

The unclear guidance and threat of fines under GDPR is an excellent example of such an unintended consequence. While INTA understands that threat of a fine is to ensure compliance, there is the unintended consequence of thwarting reasonable efforts to seek redress for those who have been harmed through abusive acts. INTA recommends that interpretative guidance be developed that takes business interests into consideration. For example, what constitutes acceptable practice for achieving balance between protecting the interests of data subjects and the interests of businesses engaging in international trade. The necessary balancing would focus on the rights of a data subject to limit access to and use of his/her data against the rights of a business to access and use the data for a legitimate purpose, whether that is to provide goods and services or to protect the intellectual property rights of the business. When a business’ intellectual property rights are threatened, the business needs to have the ability to determine the identity of the infringing party. Third parties should be given an incentive to assist in enforcement of legitimate claims and not be fearful of burdensome fines under an unclear statute.

II.6 - THE E-COMMERCE DIRECTIVE ALSO PROHIBITS MEMBER STATES FROM IMPOSING ON INTERMEDIARY SERVICE PROVIDERS' GENERAL MONITORING OBLIGATIONS OR OBLIGATIONS TO SEEK FACTS OR CIRCUMSTANCES OF ILLEGAL ACTIVITIES CONDUCTED ON THEIR SERVICE BY THEIR USERS. IN YOUR VIEW, IS THIS APPROACH, BALANCING RISKS TO DIFFERENT RIGHTS AND POLICY OBJECTIVES, STILL APPROPRIATE TODAY? IS THERE FURTHER CLARITY NEEDED AS TO THE PARAMETERS FOR 'GENERAL MONITORING OBLIGATIONS'? PLEASE EXPLAIN.

The Digital Services Act needs to strike the right balance to monitor all activity, versus the efficacy in requiring steps to detect specific infringement, which has been found not to constitute general monitoring.

IV. 14 - BASED ON YOUR EXPERIENCE, WHAT ACTIONS AND GOOD PRACTICES CAN TACKLE THE PLACEMENT OF ADS NEXT TO ILLEGAL CONTENT OR GOODS, AND/OR ON WEBSITES THAT DISSEMINATE SUCH ILLEGAL CONTENT OR GOODS, AND TO REMOVE SUCH ILLEGAL CONTENT OR GOODS WHEN DETECTED?

As mentioned in preceding questions, INTA has published best practices for search engine advertisements in Addressing the Sale of Counterfeits on the Internet. These guidelines serve as a roadmap for voluntary collaboration between search websites, online marketplaces, payment service providers, and trademark owners, as well as of social media, logistics, registrars and registry companies. INTA is currently updating this document and will provide updates to the Commission as it is completed.

Search engine advertisements appearing in search engine results page provide a way for advertisers to communicate information to users relevant to their queries. Some bad actors exploit such advertising services to promote the sale of counterfeit goods. Search engine advertising platforms generally have policies against counterfeits. Some have even developed complex engineering methods to detect and root out advertisers that use tactics indicating fraud, including by counterfeiters. To the extent that a counterfeiter evades such proactive measures, search engine advertising platforms should provide trademark owners an easy-to-use reporting process and swift action on valid reports including the following:

- Applicable terms of service or other policies should expressly and clearly prohibit advertisements promoting counterfeit goods by advertisers using search engine advertising services; search advertising services should enforce these terms and policies.
- Search advertising services should have a clear and effective complaint process publicly available to report counterfeit ads. Such process shall specify, at a minimum, the information required to be reported by the trademark owner, which shall not be unduly burdensome. Search advertising services should furnish timely and effective responses to such reports that conform to their stated process requirements.
- Trademark owners and search advertising services should work collaboratively in an open, consultative exchange to target counterfeit ads.
  - Examples of such collaboration may include trademark owners' sharing with search advertising services new tactics or trends by counterfeiters targeting the trademark owners' brands.

- Determining the most appropriate technique(s) for targeting counterfeit ads may vary depending on the facts, bearing in mind that:
  - The trademark owner has greater insights into
    - Its own trademarks (particularly those that are not famous or well known);
    - Common abuses of its marks and products/services;
    - Identifying counterfeit versions of its products; and
    - Identifying recidivist counterfeiters of its brand.
  - The search advertising services has greater insights into
    - The technological issues inherent in any attempt to accurately target and combat problematic categories of abuse, such as counterfeiting, including:
      - Filtering and blocking can sweep too broadly and encompass legitimate results; and
      - Massive resources are needed to develop and stay current with such technology;
    - The technological issues involved in correctly identifying a user of any online service, even when a search advertising service has a contractual relationship with that user;
    - The enormous volume of users of any given search advertising services;
    - Business resistance to resource-intensive "fixes" when such "fixes" have not been shown to have the effect of reducing or deterring abuse; and
    - Identifying recidivist counterfeiters reported by multiple brands.
- Search advertising services should take steps on an ongoing basis (through forums such as INTA) to educate trademark owners as to their policies and procedures for dealing with counterfeiting abuse.

Advertising is often the economic engine that supports sites dedicated to disseminating counterfeit goods and services. A variety of measures are in place that in combination, go some way to addressing this issue. These include:

- Site blocking legislation which has been implemented in various countries such as the UK, Singapore and Australia is another useful tool to deal with illegal content and goods detected outside countries which make action and enforcement difficult.

- Local competition authorities which take action at their election and on behalf of consumers also provide an alternative means of policing the local marketplace, prosecuting and penalizing companies who breach local advertising standards. A recent example is the Australian Competition and Consumer Commission (ACCC) prosecution of HealthEngine, in relation to edited and deleted negative reviews in violation of the Australian Consumer Law which resulted in significant fines. The ACCC has also taken action against internet advertisers in relation to misleading online ads e.g. *Australian Competition and Consumer Commission v ABG Pages Pty Ltd* ([2018] FCA 764)), in which the advertiser conceded that it had engaged in unconscionable conduct by misleading potential customers about the number and nature of the businesses which had been advertised on its directory and the Federal Court of Australia imposed significant penalties as a result.

Otherwise, company policies and approaches to governance that prohibit ads in conjunction with illegal content and goods provide a useful baseline mechanism to deal with this issue.

Legislative measures would only make sense if it were established that the advertiser is specifically directing a placement agent or the content provider to place the ad next to the illegal content. If, on the other hand, the advertiser can show that he has no influence over the content his ad is being placed to, this measure would certainly be disproportionate. A disclaimer by the platform advising on the possibility of such liability would not necessarily have any effect on the advertiser's placement policy.

ONE OTHER GENERAL POINT

More creative and effective efforts need to be done to fight counterfeiting, especially given its galloping development and the risk it represents for consumers. Every single stakeholder should be actively involved, whether from the public or the private sector.

INTA acknowledges that finding the right balanced and efficient approach is not an easy equation to solve. Many factors need to be taken into account including: the complexity and multiplicity of the stakeholders involved; the difference of the services and actions stakeholders can be reasonably asked to take; the potential side effects on a stakeholder's business; the available and future technologies that can help; the need to take into account the jurisprudence so carefully developed so far; and the specificity of certain scenarios which make it difficult to adopt a one-size fits all approach. INTA therefore greatly appreciates the opportunity to participate in this public consultation, which will go far in helping to understand this complex equation before trying to solve it.

* * *

For any questions, please reach out to Maysa Razavi, mrazavi@inta.org, Manager, Anticounterfeiting, and Lori Schulman, Senior Director, Internet Policy, lschulman@inta.org.

About INTA: the International Trademarks Association (INTA) is a global association of brand owners and professionals dedicated to supporting trademarks and related intellectual property (IP) to foster consumer trust, economic growth, and innovation. As a not-for-profit association, our role is to serve our members, the profession, and society as a trusted and influential advocate for the economic and social value of brands. Our membership comprises nearly 6,500 organizations from 185 countries. The organizations represent more than 34,350 professionals, including brand owners from major corporations, small- and medium-sized enterprises, law firms, and nonprofits. Our community also includes government agency members, professors, and law students. More on www.inta.org