## I. Background information

1. Please indicate your role for the purpose of this consultation: Single choice reply (compulsory)
   - Intellectual property rights holder - Business federation

2. Please indicate your place of residence or establishment: Single choice reply (compulsory)
   - Belgium

3. Please provide your contact information (name, address and e-mail address): Open reply (compulsory)
   - Christina Sleszynska, Europe Representative International Trademark Association (INTA) Level 21 - Bastion Tower Place du Champ de Mars 5 B-1050 Brussels - Belgium +32-2-550-3833, f: +32-2-550-3535 csleszynska@inta.org. For more information about INTA, please visit www.inta.org

4. Is your organisation registered in the Interest Representative Register: Single choice reply (compulsory)
   - Yes

5. What is / are the category /ies of illegal content of greatest relevance to you in the context of N&A procedures: Multiple choice reply (compulsory)
   - Infringements of trademarks

## II. Notice and Action procedures in Europe

<table>
<thead>
<tr>
<th>Statement</th>
<th>Opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action against illegal content is often ineffective</td>
<td>No opinion</td>
</tr>
<tr>
<td>Action against illegal content is often too slow</td>
<td>No opinion</td>
</tr>
<tr>
<td>Hosting service providers often take action against legal content</td>
<td>No opinion</td>
</tr>
<tr>
<td>There is too much legal fragmentation and uncertainty for hosting service providers and notice providers</td>
<td>No opinion</td>
</tr>
<tr>
<td>The exact scope of ‘hosting’ is sufficiently clear</td>
<td>No opinion</td>
</tr>
<tr>
<td>The terms “actual knowledge” and “awareness” are sufficiently clear</td>
<td>No opinion</td>
</tr>
<tr>
<td>The term “expeditiously” is sufficiently clear</td>
<td>No opinion</td>
</tr>
</tbody>
</table>
The public consultation on e-commerce of 2010 has demonstrated that most stakeholders consider hosting of websites to be hosting, but that there is less unanimity on other services that could be hosting. The CJEU has stated that hosting may in principle be the services of online market places, referencing services and social networks.

8. In your opinion, what activities should be considered as 'hosting'?

- multiple choices, reply (compulsory)

III. Notifying illegal content to hosting service providers

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is easy to find pages or tools to notify illegal content</td>
<td>No opinion</td>
</tr>
<tr>
<td>It is easy to use pages or tools to notify illegal content</td>
<td>No opinion</td>
</tr>
<tr>
<td>10. Should all hosting service providers have a procedure in place which allows them to be easily notified of illegal content that they may be hosting?</td>
<td>Yes</td>
</tr>
<tr>
<td>Some hosting service providers have voluntarily put in place mechanisms to receive notifications of illegal content. Some of these providers have complained that their mechanisms are not always used and that concerns about content are not notified in a manner that would be easy to process (e.g. by fax, without sufficient information to assess the alleged illegal character of content etc.). Providers also claim that this creates delays in taking action against illegal content, because the hosting service provider would for instance have to contact the notice provider to ask for additional information.</td>
<td>No opinion</td>
</tr>
<tr>
<td>11. If a hosting service provider has a procedure for notifying illegal content (such as a web form designed for that purpose) that is easy to find and easy to use, should illegal content exclusively be notified by means of that procedure?</td>
<td>Yes</td>
</tr>
<tr>
<td>A notice should be submitted by electronic</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>means</strong> - single choice reply - (compulsory)</td>
<td></td>
</tr>
<tr>
<td>A notice should contain contact details of the sender - single choice reply - (compulsory)</td>
<td>Yes.</td>
</tr>
<tr>
<td>A notice should make it easy to identify the alleged illegal content (for instance by providing a URL) - single choice reply - (compulsory)</td>
<td>Yes.</td>
</tr>
<tr>
<td>A notice should contain a detailed description of the alleged illegal nature of the content - single choice reply - (compulsory)</td>
<td>Yes.</td>
</tr>
<tr>
<td>A notice should contain evidence that the content provider could not be contacted before contacting the hosting service provider or that the content provider was contacted first but did not act - single choice reply - (compulsory)</td>
<td>Yes.</td>
</tr>
<tr>
<td>Both civil rights organisations and hosting service providers have complained about a significant proportion of unjustified or even abusive notices. Some stakeholders have proposed more effective sanctions and remedies for this purpose.</td>
<td>No opinion</td>
</tr>
<tr>
<td>13. Should there be rules to avoid unjustified notifications? - single choice reply - (compulsory)</td>
<td></td>
</tr>
<tr>
<td>14. How can unjustified notifications be best prevented? - multiple choices reply - (compulsory)</td>
<td>No opinion</td>
</tr>
</tbody>
</table>

### IV. Action against illegal content by hosting service providers

| 15. Should hosting service providers provide feedback to notice providers about the status of their notice? - single choice reply - (compulsory) | Yes |
| Multiple choice - multiple choices reply - (compulsory) | The hosting service provider should send a confirmation of receipt. - The hosting service provider should inform the notice provider of any action that is taken. |
| 16. Should hosting service providers consult the providers of alleged illegal content? - single choice reply - (compulsory) | No opinion |
| According to the E-commerce Directive, the hosting provider should act "to remove or to disable access to the information" - One may interpret "removing" as permanently | No opinion. |
taking down or deleting content. “Disabling access” can be understood as any technique that ensures that a user does not have access to the content. Some hosting service providers for instance use geo-software to impede access exclusively to users with an IP address from a country where the content is question is considered illegal. Similarly, some hosting service providers firstly impede access to all users without permanently deleting it. This can for instance allow law enforcement authorities to further analyse the alleged illegal content in the context of criminal investigations. If deleting would not any longer hinder the investigation, the hosting service provider may still remove the content.

17. Assuming that certain content is illegal, how should a hosting service provider act? 

<table>
<thead>
<tr>
<th>Single choice reply (compulsory)</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Several providers may host the same content on a particular website. For instance, a particular ‘wall post’ on the site of a social network may be hosted by the social network and by the hosting service provider that leases server capacity to the social network. It may be that this hosting service provider that leases server capacity is in a position to act against the alleged illegal content, but not without acting against other (legal) content.</td>
<td></td>
</tr>
</tbody>
</table>

18. When the same item of illegal content is hosted by several providers, which hosting service provider should act against it? 

<table>
<thead>
<tr>
<th>Single choice reply (compulsory)</th>
<th>As fast as possible depending on the concrete circumstances of the case</th>
</tr>
</thead>
<tbody>
<tr>
<td>As soon as the illegal nature of certain content has been confirmed, the E-commerce Directive requires the hosting service provider to act “expeditiously” if the provider is to be exempted from liability. However, the Directive does not further specify the concept of &quot;expeditiously&quot;. Some stakeholders consider that a pre-defined timeframe for action should be established, whereas others consider that the required speed of action depends on the circumstances of the specific case. In a specific case it may be difficult to assess the legality of content (for example, if the content is of a political nature).</td>
<td></td>
</tr>
</tbody>
</table>

instance in a case of defamation) or it may be easy to do so (for instance in a manifest case of child abuse content). This may have an impact on the speed of action. Similarly, what is expeditious for a specific category of content may not be sufficiently expeditious for another. For instance, the taking down of content within 6 hours will generally be considered very fast, but may not be sufficiently fast for the live-streaming of sports events (that are not any longer relevant once a match is finished).

19. Once a hosting service provider becomes aware of illegal content, how fast should it act?
   - single choice reply (compulsory)
   - In individual cases, law enforcement authorities may ask hosting service providers not to act expeditiously on certain illegal content that are the subject of criminal investigations. Acting expeditiously could alert law enforcers of the existence of a criminal investigation and would impede analysing the traffic on a particular site.

20. Should hosting service providers act expeditiously on illegal content, even when there is a request from law enforcement authorities not to do so? - single choice reply (compulsory)
   - Civil rights organisations complain that hosting service providers sometimes take down or disable access to legal content. They claim that some hosting service providers automatically act on notices without assessing the validity of the notices. In this context, the CJEU has held that blocking of legal content could potentially undermine the freedom of expression and information.

21. How can unjustified action against legal content be best addressed/prevented? - multiple choices reply (compulsory)
   - Some hosting service providers are hesitant to take proactive measures to prevent illegal content. They claim that taking such measures could be interpreted by courts as automatically leading to "actual knowledge" or "awareness" of all the content that they host. This would accordingly lead to a loss of the liability
exemption they enjoy under the respective national implementation of the E-commerce Directive. In at least one national ruling, a court has interpreted actual knowledge in this sense. At the same time, the CJEU has held that awareness can result from own initiative investigations (Judgment of the Court of Justice of the European Union of 12 July 2011 in case C-324/08 (L’Oréal – eBay), points 121-122).

22. In your opinion, should hosting service providers be protected against liability that could result from taking pro-active measures? -single choice reply-(compulsory)

VI. The role of the EU in notice-and-action procedures

23. Should the EU play a role in contributing to the functioning of N&A procedures? -single choice reply-(compulsory) Yes

Please specify: -multiple choices reply-(compulsory) By encouraging self-regulation

Article 14 of the E-commerce Directive does not specify the illegal content to which it relates. Consequently, this article can be understood to apply horizontally to any kind of illegal content. In response to the public consultation on e-commerce of 2010, stakeholders indicated that they did not wish to make modifications in this regard.

24. Do you consider that different categories of illegal content require different policy approaches as regards notice-and-action procedures? -single choice reply-(compulsory) Yes

Please clarify giving concrete examples relating to the question above -open reply-(optional)

VII. Additional comments

25. Do you wish to upload a document with additional comments? -single choice reply-(optional) Yes
Annex: INTA’s response to Notice-and-Action consultation

**Question 10:*** INTA would like to share its paper on addressing the sale of counterfeits on the Internet and best practices for voluntary measures in addressing the sale of counterfeits on the Internet.

**Addressing the Sale of Counterfeits on the Internet**

**The Issue**

In the global environment, the sale of counterfeit goods remains a significant issue facing consumers, industry and governments alike. The advent and subsequent rapid development of the Internet has raised the problem to heightened levels as counterfeiters find simplified means and additional channels in cyberspace to promote and sell counterfeit products to consumers.

A number of key factors have spurred the growth of counterfeit sales online:

- **Worldwide reach** of the Internet means that sellers of counterfeits can reach consumers all over the world and are not limited to "brick and mortar" establishments. Likewise, consumers who have access to the Internet are more exposed to and have more opportunities to knowingly or unknowingly purchase counterfeits from sellers within or outside their respective countries.

- **Payments can be made entirely online.** Therefore, it is not only consumers who can purchase counterfeits using the Internet; retailers, wholesalers, re-sellers or anyone else with a credit card can shop for counterfeits online.

- **The anonymity gained from operating via the Internet allows counterfeiters to more easily dupe consumers into thinking they are buying genuine products.** A number of factors contribute to this:
  
  - Entering a trademark owner’s trademark into a search engine does not guarantee that each website in the search results (whether in the natural results or the sponsored links) offers only genuine products of the trademark owner. Online sellers of counterfeit, like online sellers of genuine branded products, can take steps to achieve higher listings for their websites in the natural results and (under current U.S. law in at least some jurisdictions) purchase a trademark owner’s trademark as a keyword to secure a listing in the sponsored results. Online purchasers seeking to buy genuine products — and intending to pay for genuine products — may instead receive links to sites selling counterfeits.
  
  - Internet sellers can easily post pictures showing genuine products, but then ship
counterefts to those consumers once the sale is placed online. This is in contrast to sales at brick-and-mortar stores, where consumers can see and handle the product they are purchasing.

The Impact

Increased sales and access to counterefts pose serious threats to the economy and to public health and safety. The Organization for Economic Cooperation & Development ("OECD") noted in the recent study on "The Economic Impact of Counterfeiting and Piracy" that the Internet has provided counterefters with a new and powerful means to sell their products, suggesting that a significant share of the countereft trade is attributable to the Internet.\(^1\) Public health and safety are put at grave risk by countereft pharmaceuticals, airplane and automotive parts and electronic goods that are made with substandard and/or toxic materials.

It has also facilitated counterefting activities conducted by organized criminals. The OECD report shows that criminal networks and organized crime thrive via counterefting and piracy activities.\(^2\) U.S. authorities have reported that sales of countereft goods, including fake medicine, have been used to support the Middle-Eastern terrorist group Hezbollah.\(^3\) Counterefting proceeds have been linked by other investigators to Al-Qaeda, the Irish Republican Army, ETA, the Mafia, Chinese Triad gangs, the Japanese Yakuza crime syndicates, Russian organized criminals and international illegal drug cartels.\(^4\)

The Discussions

While the link between the increased sales of counterefts on the Internet and the harms caused to businesses and the public is clear, the solution to the issue is complex and challenging. As a result, how to address the sale of counterefts on the Internet has become a hotly debated topic within industry and policy-makers, alike. Questions on who is responsible for curbing the problem and what legal, policy and/or voluntary measures are needed have been widely discussed in industry and government forums. Measures to address the issue are under consideration at the international level, such as the Anti-Counterefting Trade Agreement (ACTA) – a plurilateral trade agreement with the objective of raising standards in combating counterefting and piracy.

Counterfeit sales over the Internet have become a priority for INTA. After in-depth study and

---

1 OECD, "The Economic Impact of Counterfeiting and Piracy – Executive Summary"
2 OECD, "The Economic Impact of Counterfeiting and Piracy – Executive Summary"
3 Id.
4 Carratu International, Plc, "Rise in Countereft Market Linked to Terrorist Funding," June 26, 2002
debate over several years, INTA’s Anti-Counterfeiting and Enforcement Committee (ACEC) presented its analysis and initial recommendations to INTA’s Board in 2008. As a result, two task forces were formed to examine and develop recommendations on practical ways for trademark owners, online marketplaces, search websites and payment service providers (PSPs) to address the sale of counterfeits over the Internet. One task force was comprised of online marketplace and search websites, while the other task force was comprised of PSPs. Trademark owners who are victims of online counterfeiting participated in both task forces.

The task forces explored ways for trademark owners and online service providers to work cooperatively to address the sale of counterfeits over the Internet. The end result was the development of voluntary best practices for trademark owners and Internet-related companies aimed at facilitating the protection of trademarks on the Internet. These best practices were presented to the INTA Board in May, 2009.

One important outcome of the best practices is that contact information for online service providers has been provided for use when notifying them of sales of counterfeits on the Internet — an important course of action for trademark owners attempting to take down or disrupt the sale of these illegal products. Yahoo!, eBay, Google, American Express, MasterCard, Visa, Discover and PayPal were among those who participated in and contributed contact information to the best practices.

**Future Considerations**

Addressing the sale of counterfeits online will continue to be challenging and complex. The Internet is unquestionably changing the way commerce and business is being conducted around the world. Continued technological advances and innovations mean that the Internet will evolve and allow sellers and buyers to interact in multiple ways in the virtual world. Furthermore, differences in business models and operations of Internet Service Providers (ISPs), search engines and other online players as well as trademark owners make it challenging to develop one solution to tackle the entire problem.

To be sure these voluntary measures will need to evolve in order to adapt to the changing virtual and technological environment. INTA will be looking for opportunities to promote adoption of the best practices and gain member feedback on their usefulness. INTA sees the best practices as a valuable first step towards bringing together the stakeholders - online marketplaces, shopping services, search sites, payment service providers and trademark owners – so that they can begin to effectively cooperate in the effort to combat the sale of counterfeits on the Internet.

**Contact**

Candice Li, External Relations Manager – Anti-Counterfeiting
Email: cli@inta.org
Best Practices for Voluntary Measures in Addressing the Sale of Counterfeits on the Internet

Best Practices for Search Sites

1. Applicable terms of service, content and other guidelines should expressly and clearly prohibit counterfeiting activities by advertisers and other users of search engine services; search engines should actively enforce these terms and guidelines.

2. Additional appropriately placed warnings and/or reminders should be considered.

3. Search engines should have a clear and effective process publicly available to deal with counterfeiting abuse. Such process shall specify, at a minimum, the information required to be reported by the trademark owner, which shall not be unduly burdensome; when, where and how such information is to be reported; and the process by which and time frame within which the search engine will act upon such reports. Search engines should furnish timely and effective responses to such reports that conform to their stated process requirements.

4. Trademark owners and search engines should work collaboratively in an open, consultative exchange to target counterfeiting abuse that may take place within a given search engine’s services.

   • Examples of such targeting might include blocking or flagging for heightened review certain suspect terms that may be indicative of counterfeiting activity.

5. Determining the most appropriate technique(s) for targeting abuse may vary depending on the facts, bearing in mind that:

   • the trademark owner has greater insights into:

      – its own trademarks (particularly those which are not famous or well-known),
      – common abuses of its marks, products/services,
      – identifying counterfeit versions of its products, and
      – identifying recidivist counterfeitters of its brand.

   • the search engine has greater insights into:

      – the technological issues inherent in any attempt to accurately target and eliminate problematic categories of abuse, such as counterfeiting, including:

         o filtering and blocking can sweep too broadly and encompass legitimate results


- 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 the search engine has a contractual relationship with that user

- the enormous volume of users of any given search engine’s services, which makes timely and accurate manual – or even automatic - processing of ads, complaints, etc. extremely difficult

- business resistance to resource-intensive “fixes” when such “fixes” have not been shown to have the effect of reducing or deterring abuse

- identifying recidivist counterfeiters of multiple brands based on activities on the search engine’s website.

6. Search engines 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.

Best Practices for Marketplace and Shopping Sites

1. Marketplace and shopping sites shall take steps to educate their users, and actively discourage infringing activity, in connection with listings available through the marketplace’s and shopping site’s services.

   - For example, users offering to sell items that a marketplace or shopping site, in its discretion, believes may infringe third party rights, should be reminded (through the use of targeted click-through notices and/or click-through authenticity attestations) that the services may only be used in a way that is consistent with applicable laws and terms of service.

2. Such messaging should also advise users as to the possible consequences for violating applicable policies or laws, which may include permanent loss of access to the service and reference to appropriate law enforcement officials.

Best Practices for Payment Service Providers (PSPs)

1. Payment Service Providers (PSPs) should have policies in place prohibiting the use of their services for the purchase and sale of goods that are determined to be counterfeit under applicable law.

2. PSPs should have procedures for trademark owners to report websites (in accordance with 1(a) through 1(f) below) that use a PSP’s network to process payments for the sale
of allegedly counterfeit goods. An example of an efficient reporting procedure includes, but is not limited to, a single email address or online reporting form through which trademark owners can submit allegations of counterfeit sales activity.

3. Upon receipt of at least 1(a) through 1(f) (set forth below) from the trademark owner, and after a reasonable period of time for review, PSPs may provide (or may request that others provide, as appropriate) reasonable feedback to the trademark owners with respect to its findings.

4. PSPs may reserve the right to allow the website owner/operator to respond to the allegations and/or cure the alleged violation prior to responding to the trademark owner or making a determination on appropriate remedies.

5. If a PSP observes repeated violations of the PSP’s policies and applicable trademark laws through the use of its payment service, PSPs may choose to impose appropriate remedies in accordance with their own internal procedures, including, for example, termination of service.

Best Practices for Trademark Owners

Relating to Search, Online Marketplace, and Shopping Sites

1. Trademark owners should take steps on an ongoing basis to educate the public as to their trademarks.

Relating to PSPs

1. In working with PSPs on combating online sales of counterfeits, the trademark owners should provide the following information such as:

   a. A detailed description of the transactions alleged to be illegal;
   b. Information identifying the website where the alleged transactions occurred;
   c. Evidence that the alleged counterfeit item was purchased using the PSP’s services;
   d. Proof of ownership of a registered trademark in one or more of the applicable jurisdictions;
   e. A representation that the sale of the counterfeit goods at issue will cause damage to the trademark owner; and
   f. A description of the trademark owner’s good faith efforts to resolve the issue directly with the seller of the alleged counterfeit goods (or an explanation as to why such efforts have not been made).

2. The trademark owners should agree to indemnify and hold harmless the PSP (and, as applicable, other involved parties) against all liability for monetary damages, costs and attorneys’ fees awarded to sellers of alleged counterfeit goods for unlawful termination of the PSP’s services resulting from the trademark owner’s complaint.
3. If trademark owners try to make a purchase using a PSP’s services and are unable to do so notwithstanding the appearance of the PSP’s trademark on the website, the trademark owners are encouraged to report that potential misuse of the PSP’s trademark to the PSP.

CONTACT INFORMATION FOR COMPLAINTS TO PARTICIPATING PSPs*

American Express  
trademarkabuse@aexp.com

MasterCard  
abuse@mastercard.com

Visa  
Inquiries@visa.com

Discover  
RiskOperations@discover.com

PayPal  

*This list is current as of August 3, 2009

CONTACT INFORMATION FOR COMPLAINTS TO PARTICIPATING INTERNET PLAYERS

eBay, Inc.  
copyright@ebay.com

Yahoo!, Inc.  
Trademarkconcern-ysm@yahoo-inc.com

Google (http://services.google.com/inquiry/aw_counterfeit)