European Commission
DG Communication Networks, Content & Technology
Unit B2 – Regulatory coordination & users
Avenue de Beaulieu 33, 06/068
B-1049 Brussels

E-Mail: CNECT-PLATFORMS-CONSULTATION@ec.europa.eu

Vienna, 18th December 2015

ISPA ADDITIONAL CONTRIBUTION TO THE PUBLIC CONSULTATION ON THE REGULATORY ENVIRONMENT FOR PLATFORMS, ONLINE INTERMEDIARIES, DATA AND CLOUD COMPUTING AND THE COLLABORATIVE ECONOMY

Dear Sir/Madame,

ISPA (Internet Service Providers Austria; Identification Number: 56028372438-43, Contribution Case ID: 04ddc884-79ee-4ac8-8d0e-ed7440750c65) is pleased that the European Commission has issued this public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy and would like to submit some additional comments to its online reply to the survey:

- **As a holder of rights in digital content protected by copyright have you faced any of the following circumstances:**

As we haven't answered YES to any of the questions, we would like to add some comments:

The online services listed in the proposed definition of platforms are diverse in nature, ranging from online content stores to e-commerce websites. They may allow users to sell second-hand goods as e.g. DVDs, enable the online distribution of films, music or books, host videos online or allow users to share photos.

Depending on the situation, a licence, permission, exception, or application of the E-commerce liability regime may be considered. As a result, ISPA is of the opinion that it is neither appropriate nor possible to adopt a one-size fits all answer to the questions listed.

In addition, the assessment whether a commercial transaction such as licence is "fair," is a subjective test (the recent Directive 2014/26/EU already lays down different criteria in the specific case of collecting society). ISPA thus suggests to look for evidence of market failures first. If any can be found it shall be assessed from a regulatory perspective, whether the current framework is effective and proportionate. Such notions of evidence based legislation are tried and tested cornerstones for EU intervention. ISPA believes that the current framework is effective and

proportionate, although the current very complex licensing framework[1], the existence of copyright levies or the creation of new compensation claims or rights for news publishers distort markets and may themselves lead to market failure.

Many services listed in the questions above are not themselves "using" copyright works but are instead information society services coming under the scope of the E-commerce Directive. Users of such services may potentially infringe copyright - a decision ultimately for a court - in which case online services act expeditiously. The current system in our opinion strikes a good balance for all parties, including for rights owners, who gather revenue and market insights from these services.

- **If you own/develop an online platform, what are the main constrains that negatively affect the development of your online platform and prevent you from extending your activities to new markets in the EU?**

The fragmentation of rules governing the digital economy across 28 member states creates challenges to building and scaling Internet businesses across Europe. Rules around issues like copyright, including levies and cumbersome licensing processes, consumer protection, postal regulations and privacy create barriers to building a pan-European business.

Uncertainty in the legal regime also discourages investment in European digital businesses and drives many digital companies to choose to scale outside of Europe rather than across Europe. To encourage the growth of European platforms, ISPA sees a need for clear, consistent rules around liability. More self-regulation and best-practice sharing would benefit innovation.

- **Have you encountered situations suggesting that the liability regime introduced in Section IV of the E-commerce Directive (art. 12-15) has proven not fit for purpose or has negatively affected market level playing field?**

Please describe the situation.

The E-commerce Directive's liability regime has proven itself effective and proportionate, and promoted dynamic, competitive, markets since its inception. It gives online service providers the confidence to provide their services.

The Directive enables them to operate efficient, open platforms where users and third parties can exchange goods, services, and information. A recent study from Copenhagen Economics[2] [3] argues that the limited liability regime is not only necessary for the functioning and growth of online intermediaries, but is also beneficial to the European economy.

[1] ISPA study, Wiebe (Ed.) "Legal and practical problems of rights clearance from the perspective of a content provider and alternative models", 2014

[2] http://www.copenhageneconomics.com/dyn/resources/Publication/publicationPDF/6/226/0/The%20impact%20of%20online%20intermediaries%20-%20April%202013.pdf , 2.

Copenhagen Economics estimates that online intermediaries' activities in the EU contributed around €430 billion to the GDP of the EU27 in 2012. This is comprised of a direct GDP contribution of €220 billion and a long-term indirect GDP contribution due to the productivity impact of intermediaries on other firms of €210 billion. If the market level playing field is affected, it is by platforms located (or hiding) in exotic countries that provide a service within Europe (e.g. pirate sites, counterfeit marketplaces, etc.).

- **Do you think that further categories of intermediary services should be established, besides mere conduit/caching/hosting and/or should the existing categories be clarified?**

Please provide examples

With all arguments considered, retaining the status quo on the liability regime of the E-commerce Directive is the best option to allow businesses and consumers to benefit from further growth and innovation in the digital economy.

Same is true for the debate as to whether to revisit the existing categories of intermediary services. In fact, the key advantage of the E-commerce Directive is its technological neutrality, making it able to adjust to new developments on the market. The directive does not list specific business models, instead laying down a resilient, future proof model.

There is no doubt that technologies have evolved and that some intermediaries have more capacity of action, for example, providers offering mailing services may apply mechanism to reject spam messages so that their users are not flooded with unwanted messages. However this does not change the rationale of the intermediaries' liability regime. In other words, it's not because these providers can decrease the number of unsolicited mails that they can or under any condition should become liable for all forms of content they carry.

Diverging case law at the national level is due to local legal specificities that arguably are not compatible with the principles of the e-commerce directive, for example the peculiar duty of care ("Störerhaftung") regime in Germany.

- **Do you think that any of the following categories of illegal content requires a specific approach:**

  - ☐ Illegal offer of goods and services (e.g. illegal arms, fake medicines, dangerous products, unauthorised gambling services etc.)
  - ☐ Illegal promotion of goods and services
  - ☐ Content facilitating phishing, pharming or hacking
  - ☐ Infringements of intellectual property rights (e.g. copyright and related rights, trademarks)
  - ☐ Infringement of consumer protection rules, such as fraudulent or misleading offers
  - ☐ Infringement of safety and security requirements
  - ☐ Racist and xenophobic speech
  - ☐ Homophobic and other kinds of hate speech
  - ☐ Child abuse content
  - ☐ Terrorism-related content (e.g. content inciting the commitment of terrorist offences and training material)
  - ☐ Defamation
  - ✓ Other:

*Please specify.

It is important not to modify the uniform horizontal application of article 14 of the E-commerce Directive. Certain types of content may be more easily identified as illegal (e.g., child abuse content), while others require difficult legal judgments which cannot be left to the discretion of an intermediary and hence require judicial determination.

Please explain what approach you would see fit for the relevant category.

Under the liability system of the E-Commerce Directive and its case law, intermediaries must take action when the content is obviously unlawful. In Austrian the Supreme Court of Civil matter has established the criteria of “obviousness to a lay” as the respective threshold. This is a good rule, as intermediaries are private entities and are not in position to arbitrate complex legal situations.

Thus the E-commerce Directive already distinguishes between content that obviously requires immediate action (e.g. CSAM) and other content. This approach is more effective and rational than distinguishing between different categories or types of illegal content.

There is no need to implement a specific approach for single or several of the categories listed above, as intermediaries have developed their own policies, or adhered to codes of conduct, under which remedies can be provided that are broader than could be prescribed by law e.g. global removal of copyright infringing content.

- **Could you estimate the financial costs to your undertaking of putting in place and running this system?**

Documentation on costs of such systems is rare, but the few figures that exist show that they are indeed expensive. YouTube is one of the rare intermediaries which discloses how much it spent in developing Content ID: 60 million USD for a system that works just for copyright. An Irish court estimated that a software to send notices to users of an intermediary would cost between 800.000 and 940.000 Euros.

- **Could you outline the considerations that have prevented you from putting in place voluntary measures?**

Voluntary systems for notice and action, flagging systems, manual review systems, and other content monitoring/optimization and moderation systems aimed at preventing illegal content, or content that violates terms and conditions of service, should not be counted against the intermediary, when considering whether the activities of an intermediary are of a merely technical, automatic and passive nature, or whether the intermediary has knowledge of or control over the data which is transmitted or stored.

As mentioned above that the adoption of such pro-active measures should not be used as the basis for denying the intermediary the benefit of the limitation of liability set out in the E-commerce Directive. Otherwise, intermediaries would obviously be incentivised to take a hands-off approach and do nothing, thus saving the costs of development and maintenance as well as risks related to the enforcement of these measures as they can be overreaching and affect third parties.

- **Do you think that there are particular reasons in relation to which data location restrictions are or should be justifiable?**

Security is a fundamental concern when determining where to store and how to transfer data.

Yet data localization requirements increase data security risks and costs by requiring storage of data in a single centralized location that is more vulnerable to natural disaster, intrusion, and surveillance.

Data localization requirements make it more difficult to implement best practices in data security - including redundant geographic storage of data and the usage of distributed security solutions such as sharding and obfuscation.

Storing data in a single centralized location can also present a more attractive target for surveillance.

- **What information relevant to the security and protection of users' data do you think cloud service providers should provide?**

As explained below in greater detail, cloud service providers are already regulated sufficiently with regard to security and protection of users' data. When cloud service providers process personal data, they are already under the transparency requirement of the 95/46/EC and will be under similar requirements under the General Data Protection Regulation. ISPA also notes that this legislation contains the obligation of securing personal data in the cloud. To the extent that it is not contrary to the objective of achieving a high level security, transparency requirements thus already apply. Furthermore, the ongoing negotiations relating to the Network and Information Security Directive, show that it will be likely that cloud service providers will face new additional security obligations, notably on reporting of security breaches.

ISPA would like to reiterate that it is very thankful for this opportunity to contribute. For further information or any questions please do not hesitate to contact us.

Sincerely,

ISPA Internet Service Providers Austria

Dr. Maximilian Schubert

General Secretary

About ISPA: ISPA is the Austrian association of Internet Service Providers, representing approximately 200 ISPs. ISPA is a major voice of the Austrian Internet industry. Our goal is to shape the economic and legal framework to support optimal growth of the Internet and Internet services. We regard the use of the Internet as an important cultural skill and acknowledge the resulting socio-political responsibilities.