



**PUBLIC CONSULTATION ON THE FUTURE OF ELECTRONIC COMMERCE IN  
THE INTERNAL MARKET AND THE IMPLEMENTATION OF THE DIRECTIVE ON  
ELECTRONIC COMMERCE (2000/31/EC)**

**NOVEMBER 2010**

EuroISPA welcomes the opportunity to provide comments in relation to the E-Commerce Directive (thereafter "ECD"). As a general, introductory remark, we believe that the Directive offers a well balanced and functioning framework. The principles laid down therein showed to be the cornerstones for the development of the ICT industry in Europe. Therefore, they should be preserved. Without being overly prescriptive, the provisions in question serve to provide a secure and predictable legal base for our industries to connect European citizens to the Internet and other electronic communication platforms. Any interference in this delicate balance will bring with it an increase of burdens for legitimate commerce, creating a negative impact on innovation, distorting competition and undermining consumers' fundamental rights to privacy and free flow of information.

Instead legal uncertainty and interpretative problems occur more on the national level where the implementation of the Directive has not been done in a consistent manner. Additionally, EuroISPA considers that barriers to e-commerce can be found not in the ECD, but rather in other EU legislation.

---

**36. In your view, does the purchase and sale of copyright protected works subject to territorial rights and the territorial distribution of goods protected by industrial property rights, encourage or impede cross-border trade in information society services?**

As an initial consideration, we believe that the digital technology far from damaging IPR holders over contents rather strengthens their powers.

Digital technology allows content owners to distribute the same content through different platforms (e.g., theaters, DTV, satellite, IPTV, mobile TV, Blue Ray and DVD) and to charge different prices for the same content according to: (i) its different usage (Pay-TV vs. Free to air, PPU, etc.); (ii) the different time of fruition (different time windows as to Theaters, DVD, Television -first time, second time-, etc.); (iii) the different support over which the content is distributed (e.g., Blue Ray vs. DVD) and (iv) the different countries where content is distributed (in this case, the segmentation is performed though the different languages in which the content is distributed, by charging more the richer countries (such as Germany, France and UK) and less the poorer (i.e. Greece). Therefore, content owners have a significant power over price which is revealed, first of all, by this power to price discriminate and to maximize revenues by charging different prices for different times of releasing/fruition of the content as well as territories.

This power over price and power to discriminate is strengthened by the current collective management system, which is one of the most important impediments to the development of the Online Single Market and access to creativity. The EU should help to install a new, more efficient copyright clearance system which would help all market players to streamline transaction and management of costs. Other barriers may derive from the complexity of the licensing systems and the fragmentation of the European Internal Market.

The plurality of authors, performers and publishers, each having an ownership interest in a given work, undermines the ability of entrepreneurs to develop new business models suitable for e-commerce. This is exacerbated by the fragmentation of the rights themselves, including the right to make digital copies, performance, streaming and broadcast rights and database rights. When this is considered together with the plethora of notionally separate works that may be associated (for example, a music track, a video of a performance, the image of the performer, the soundtrack of a movie the track was used in, the video associated with that performance and associated image rights) the number of licenses an entrepreneur with a new business model may have to navigate multiply. In this respect, the availability of “blanket licenses” (i.e. covering a full global repertoire) should be explored for their potential to assist the development of cross-border trade in information society services.

Due attention should also be paid to barriers stemming from consumer protection regulations which place price-cap barriers on information society services resulting in *de facto* limitations to the types of services which may be marketed in a country through electronic communications networks.

**37. In your view, are there other rules or practices which hinder the provision or take-up of cross-border on-line services? If so, which?**

The Internet is a powerful tool which allows access to creativity and the development of new business models. However, while the ECD has proved to be a helpful framework for promoting online services, other rules and practices have erected barriers to the cross-border provision of online services. Obstacles to e-commerce can be found not in the Directive, but rather in other EU legislation, such as:

- a) **Harmonising diverging national rules on consumer protection:** the draft Consumer Rights Directive has attempted to harmonise certain key protections, to make it easier for small and medium sized enterprises to offer services across the single market. However, current discussions in the Parliament and Council risk undermining that harmonisation, and could even make e-commerce more difficult.
- b) **Reviewing the current system of managing copyright:** our industry is very interested in growing the Digital Single Market, particularly for digital content. However, we find the current system of copyright management, based on territoriality, to be restrictive and cumbersome, especially when we are faced with customer demand for content across multiple member states and multiple exploitation forms. The EU and national governments could take the lead in this, by for example allowing better access to public sector information for the creation of new services online.

- c) **Maintaining the right balance in the upcoming review of the Intellectual Property Rights Enforcement Directive:** the principles of the ECD are fundamental to the business models for Internet operators and form the backbone of our activities online. The balance of discussions should respect these principles and not undermine efforts to increase the take-up of e-commerce by consumers. Attractive legal offers of content are a more effective method for dealing with online piracy. However, in order to prevent piracy, the Commission should reconsider the extent of the economic protection granted to the copyright and a more balanced regulation of the conflict between “incentive to creation of” and “access to” contents. As a matter of fact, while nowadays it is clear the need to ensure adequate incentive to “creation”, through copyright (as without it only few contents would develop); on the other hand the consequences of an excessive time-space protection of copyright owners with respect to third parties access to contents have not been correctly considered. In this respect, it is noteworthy that also authors from the Chicago School are stating the need to revise such balance between “incentive” and “access” since “the...major cost of a property right system, ... of particular importance to intellectual property, arises from a common motive for obtaining a property right, the motive that economists refer to as <rent seeking>”<sup>1</sup>. The argument is that too much protection to the copyright owner allows the latter to exploit its monopoly rights by maximizing its profits (basically, through discrimination: see § 36, above) and that such huge profits push everybody to “run for the monopoly rent-seeking” and, eventually, to an inefficient allocation of resources (i.e. all majors try to produce a "Kolossal", due to the huge revenues in case of success; however, only one out of 100 movies becomes a blockbuster and allows revenues of tenths the investments afforded, while the money invested for the other 99 would be largely lost). It is therefore necessary a rapid shift of the balance between “access” and “incentive” in favor of access to contents (see also the points made under “f)”, below). In such case, it is likely that the investments would be allocated more properly and the cost of contents would decrease and, therefore, piracy phenomena would dramatically decrease.
- d) **Facilitating online payments:** we find that consumers choose illegal methods for accessing content for many reasons, including lack of access in their country. Another major reason is the inability or difficulty to make payments online and the lack of confidence of consumers. If new business models are to be found that can sustain modern habits of consuming content online, then new, secure and convenient ways of making small payments need to be found and fostered.
- e) **Harmonising and simplifying privacy and advertising rules:** the consistent interpretation and application of the EU privacy framework across Member States would promote e-commerce by fostering the confidence and trust of consumers and businesses in the information society. Online advertising is a key and attractive way of offering services on the Internet that delivers real value to users<sup>2</sup>. It is essential, therefore, that the legal framework for advertising recognises its importance in the e-commerce debate, and seeks out “win-win” solutions which provide a trusted and consistent environment for users and value for advertisers and companies. It is also

---

<sup>1</sup> W. LANDES - R. POSNER, *The Economic Structure of Intellectual Property*, Harvard University Press, 2003, pag. 16-foll.

<sup>2</sup> [http://iabeurope.eu/media/39559/whitepaper%20\\_consumerdrivingdigitaluptake\\_final.pdf](http://iabeurope.eu/media/39559/whitepaper%20_consumerdrivingdigitaluptake_final.pdf)

important to promote international regulatory dialogue to ensure a level playing field on a global marketplace for online advertising.

- f) **Updating the copyright exceptions and limitations regime:** The Internet is a powerful tool which allows access to creativity and the development of new business models. In the context of copyright protected works, Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society actually provides for exceptions and limitations to copyright. However, harmonisation is lacking since those exceptions and limitations are based on discretionary provisions and this has a detrimental effect on the development of online services across Europe. With the notable and crucial exception of Article 5.1 of Directive 2001/29/EC, little has been done to harmonise and adapt the exception regime to the changing needs of the information society and to ensure that it can adapt quickly to the rapidly evolving environment. The next wave of innovation and services is about to hit Europe and the industrialised world, with next-generation networks and new and developing technologies bringing the online single market into another era. It is, therefore, needed for the Commission to look again at the issue of copyright exceptions – every barrier to openness and communication that can be torn down in this process will benefit European consumers, business, innovators and the European knowledge economy<sup>3</sup>.

We also urge the Commission to put in place a strategy to implement the suggestions in the Report and Communication of 2009 on cross-border e-commerce including:

- Ensure effective enforcement of Article 20 (non-discrimination) of the Services Directive (2006/123);
- Increase the efficiency of cross-border enforcement;
- Tackle unfair commercial practices, both in B2C and B2B;
- Promote alternative dispute resolution schemes and the cross-border small claims procedure;
- Simplify the VAT reporting obligations of distance sellers;
- Reduce online businesses' administrative burden concerning waste of electrical and electronic equipment;
- Use competition rules on vertical restraints to contribute to reducing barriers to online markets;
- Strengthen market monitoring.

**52. Overall, have you had any difficulties with the interpretation of the provisions on the liability of the intermediary service providers? If so, which?**

The provision in Article 12(3) that the right of courts to issue injunctions is not impaired is causing a degree of confusion. We believe that a proper interpretation is that this right is applicable only in specific cases in respect of specific users. However, certain stakeholders have argued that this provision permits the court to impose upon mere conduits a liability to filter Internet traffic, block access to certain locations and services at the ongoing demand of

---

<sup>3</sup> See the EuroISPA's contribution to the European Commission's Green Paper on Copyright in the Knowledge Economy: [http://www.euroispa.org/files/081127\\_euroispa\\_copyright\\_green\\_paper.pdf](http://www.euroispa.org/files/081127_euroispa_copyright_green_paper.pdf)

the complainant. We do not believe that such an interpretation is acceptable as it largely would negate the effect of Article 12(1), but clarification of this point would avoid the need for litigation in which courts in Member States are (subject to appeal at least) reaching inconsistent conclusions.

In some countries, such as Italy, difficulties were faced with the interpretation of the provisions on the liability of the intermediary service providers. We wish to stress that an effort to ensure an effective enforcement of copyright in the Internal Market risks to affect the balance between the different interests at stake underlying the mentioned rules on E-commerce (Articles 12-15 ECD), with the result to seriously affect the development of E-commerce. Such issues have arisen in the context of provisions different from the E-Commerce Directive (relating to the enforcement of copyright) but are capable of distorting its application due to possible misinterpretation of such rules.

It is therefore requested to clarify definitely that: (i) ISP providing mere access to Internet (“mere conduit”) are not liable to suspend Internet access services (or access to specific sites) to their users in case of a mere warning by the owner of the copyrights allegedly affected by the ISPs’ users; (ii) that ISPs have no liability towards such owner if inertial further to its warning and (iii) that ISPs can (and shall) prevent access to their users only further orders of competent administrative bodies or of national courts.

**53. Have you had any difficulties with the interpretation of the term "actual knowledge" in Articles 13(1)(e) and 14(1)(a) with respect to the removal of problematic information? Are you aware of any situations where this criterion has proved counter-productive for providers voluntarily making efforts to detect illegal activities?**

The “actual knowledge” requirement has proven to be a cornerstone of the safer-harbor regime for both caching and hosting providers. The general wording introduced in the Directive was elaborated on purpose to ensure that the decision on the legality of a given piece of content would only be taken by a court or an administrative authority with trained personnel able to make balanced assessments. This approach proved to be useful in the prevention of active monitoring of allegedly illegal activities in compliance with the “no general monitoring obligation” in Article 15. However, the lack of a specific definition of “actual knowledge” gave rise to interpretative problems at national level concerning the exact conditions under which a service provider was effectively acquiring such knowledge. In some cases, it is unclear if the intermediary acquires actual knowledge when a user is simply making a complaint or flagging a content deemed inappropriate, as opposed to a court order or decision establishing that a piece of content is effectively illegal.

In this context several questions arise: What kind of information is necessary in order to provide actual knowledge to the intermediary? How detailed must this information be? Can this information be provided by any third party or is it necessary that it is provided by the affected party? Concerning the actual knowledge about the illegality of content, does the intermediary need to carry out a legal analysis or must such illegality be apparent for everyone?

In order to cope with such concerns and minimise the risks related to hypothesis of ignorance, purposefully disinformation or inadvertency, the provider has been generally deemed having actual knowledge of the illegal deeds once a competent authority has declared the content illegal and has ordered its withdrawal, limitation to its access or declared the existence of damages, and the service provider knew about such decision. Similar objective facts have been established, for example, by a detailed notice from a copyright owner. This, sometimes, requires service providers to address complex issues, such as whether particular acts that have been notified, such as terrorism or hate speeches allegations, are illegal or not, whether a product has been “put on the market” in the EU, is second-hand, is a tester, etc.

Actual knowledge, therefore, needs to be linked to a notification which fulfills certain minimum requirements such as:

- the notification should be in writing;
- the complainant should provide adequate identification of the specific item of content alleged to be infringing (a general description of the type of content, that requires the intermediary to investigate to discover which particular items match that description, is not sufficient);
- the notification should be sent to an e-mail address reserved for this purpose by the service provider;
- it should clearly specify which information or activity the complaint relates to;
- it should provide evidence that the complainant possesses the rights which he claims to be violated;
- it include an assertion that the publisher or person making the work available is infringing their rights and does not have a lawful basis for publishing the work or making it available (whether by means of a license or by operation of law);
- it should include details of the unlawful nature of the activity or information in question;
- it should contain an assertion of truthfulness and accuracy of the above and include an admission of liability for action taken in reliance on the same.

It is noteworthy an Italian recent case where an ISP had “actual knowledge” from a third party warning alleging infringement of copyright by the ISP’s users, through a notification meeting the above minimum requirements. The Court stated that the ISP only obligation was to forward to the competent authorities (i.e Public Prosecutor’s office and Ministry of Communications) all the information relating to the alleged infringements of copyright contained into the warning (order of Tribunal of Rome no. 415 of 2010).

### **Voluntary industry agreements**

The above does not prejudice procedures of detection and content removal that service providers might implement under voluntary agreements and other means of actual knowledge that may be established. Such procedures are voluntary mechanisms for cooperation set forth in the ECD, through which the interested party can report the existence of an alleged illegal activity to an ISP with a view to the ISP reviewing the purportedly content and, as the case may be, assessing the advisability of removing or disabling access to it.

However, EuroISPA believes that there are a number of requirements and conditions that must be considered when setting up voluntary industry agreements. The aim should also be

to reinforce legal certainty for ISPs and their liability limitations, and create the context for a true collaboration with parties to the agreement. In principle Articles 12 – 15 should not be affected by voluntary industry agreements. In particular it must be excluded that any voluntary agreements give rise to a presumption of actual knowledge that would expose the service provider to liability.

**54. Have you had any difficulties with the interpretation of the term "expeditious" in Articles 13(1)(e) and 14(1)(b) with respect to the removal of problematic information?**

Service providers must expeditiously remove, or block access to, information once they are aware of their illegal nature. The Directive does not define this requirement and leaves to Member States to "*[establish] specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information*" (Recital 46). Generally speaking, the term "expeditious" offers the necessary flexibility for case-by-case assessments. It cannot be laid down without the individual circumstances of the particular case.

If the expeditious action of a provider is due when the notice is coming from a court, a different assessment should be done in case of voluntary mechanisms. Indeed, while in the former case the intermediary has legal certainty, in the latter it could be required to act as soon as it is put on notice regardless of whether it has all the elements and the level of certainty needed to make a decision about the illegality of the content to be removed or disabled. Calling for expeditious removal in these cases, could result in the disabling access to sites or content that are not illegal, with far reaching consequences for the person unduly affected.

**55. Are you aware of any notice and take-down procedures, as mentioned in Article 14.1(b) of the Directive, being defined by national law?**

In **Finland**, notice and take down procedure is defined on the Finnish Act on Provision of Information Society Services (458/2002) (specifically sections 15, 20-25)<sup>4</sup>.

According to Finnish legislation hosting service provider is not liable for the information stored or transmitted at the request of a recipient of the service if he/she acts expeditiously to disable access to the information stored:

1. upon obtaining knowledge of the order concerning it by a court;
2. if it concerns violation of copyright or neighboring right upon obtaining the notification from the right holder;
3. upon otherwise obtaining actual knowledge of the fact that the stored information is clearly contrary to Finnish penal code Sections regarding ethnic/other incitement against group of people or unlawful pornographic pictures.

Finnish N&TD law/procedure regarding copyright infringing material in short:

---

<sup>4</sup> <http://www.finlex.fi/en/laki/kaannokset/2002/en20020458>

A holder of copyright may request hosting service provider to prevent access to material infringing copyright:

- If the content producer cannot be identified;
- if content producer does not remove the material or prevent access to it expeditiously.

The hosting service provider is not liable for the information stored or transmitted if he/she acts expeditiously to disable access to the information stored upon obtaining the notification from the right holder.

The notification must be made in writing or electronically so that the content of the notification cannot be unilaterally altered and that it remains available to the parties.

The notification must include:

1. the name and contact information of the notifying party;
2. an itemisation of the material, for which prevention of access is requested, and details of the location of the material;
3. confirmation by the notifying party that the material which the request concerns is, in his/her sincere opinion, illegally accessible in the communication network;
4. information concerning the fact that the notifying party has in vain submitted his/her request to the content producer or that the content producer could not be identified;
5. confirmation by the notifying party that he/she is the holder of copyright or neighboring right or entitled to act on behalf of the holder of the right;
6. signature by the notifying party.

The notification which does not meet the requirements is invalid.

The hosting service provider must immediately notify the content producer of prevention of access to the material supplied by him/her and to supply the content producer with a copy of the notification on the basis of which prevention was made. If the content producer considers that prevention is groundless, he/she may get the material returned by delivering to the notifying party a plea in writing or electronically, within 14 days of receiving the notification. A copy of the plea must be delivered to the service provider. The plea must include:

1. the name and contact information of the content producer;
2. the facts and other reasons under which prevention is considered groundless;
3. an itemisation of the material for which prevention is considered groundless;
4. signature by the content producer.

If the plea is delivered within the time limit, the service provider must not prevent the material specified in the plea from being returned and kept available unless otherwise provided by an agreement between the service provider and the content producer or by an order or decision by a court or by any other authority.

He/she who gives false information in the notification, is liable to compensate for the damage caused.

The hosting service provider must give a contact point where the notifications may be delivered.

In the **United Kingdom**, notice and takedown procedures are used to deal with a whole range of unlawful content online. The Ecommerce Directive was transposed through the Electronic Commerce (EC Directive) Regulations in 2002. The Regulations do not establish statutory procedures governing the removal or disabling of access to information through "notice and takedown" procedures. However, Regulation 22 of the Regulations states that for ISPs to have been put on notice the following must be included:

1. the full name and address of the sender of the notice;
2. details of the location of the information in question; and
3. details of the unlawful nature of the activity or information in question.

When an ISP is notified of the content, to avoid any liability under the ECD, upon gaining actual knowledge the ISP will expeditiously review the content and, upon review, may choose to remove the content. For child abuse content and religious and racial hatred in the UK, the Internet Watch Foundation provides notices to intermediaries.

For radicalization/terrorism content, the Terrorism Act 2006 gave powers to law enforcement to have content removed by issuing Section 3 notices. It contains a notice and takedown regime that applies to website operators. A police constable may serve a notice requiring the modification or removal of offending material within two days. The effect of any failure to remove or modify the materials within the two-day period, in the absence of "reasonable excuse," is that the service provider will be deemed to have endorsed the offending materials and faces a maximum penalty of seven years in prison. The UK ISPA and its members worked with the government to come up with guidance for issuing these notices. However, to date, no Section 3 notices have been issued by the government. Instead, informal contact between law enforcement and ISPs has been used to remove radicalization content.

However, the UK's implementation through the E-commerce Regulations 2002, does not apply to legislation after the event, so the protections need to be given on a case-by-case basis. This is known as prospective effect of the ecommerce regulations and means that each time a new piece of legislation is enacted that is relevant to online content, new regulations have to be drawn up for each piece of legislation, presenting ISPs with real risk of liability each time a new piece of legislation is passed.

In **Italy**, the "Guidelines for the adoption of codes of conduct and actions for the spreading of digital content in the Internet Age" of March 2, 2005 (known as the "Pact of San Remo"), Internet Service Providers committed to "adopt, in accordance with the provisions of d. lgs. [legislative decree] 70/2003, all efforts to ascertain the abusive electronic spreading of unlawful material for creating a secure digital environment" and "to define suspension or termination clauses of the contract with end customers, which application is dependent on the ascertainment of the copyright infringement", and rights holders have committed themselves, on their side, to "significantly increase the quantity and quality of digital content placed on the net in order to develop the online market". Moreover, in the same place, the rights holders, suppliers of connectivity and production companies and operators of distribution platforms, through their associations, have committed themselves to define and adopt codes of conduct and to send a copy to the Presidency Council of Ministers, together with any information relevant to their application.

**56. What practical experience do you have regarding the procedures for notice and take-down? Have they worked correctly? If not, why not, in your view?**

The notification procedure of allegedly illegal material for hosting providers in Article 14 ECD does not clearly define the mechanism to adopt in order to establish “actual knowledge” or “awareness of facts or circumstances”. As consequence, diverging approaches have been adopted across Member States which could be gathered in the following categories:

1. **A formal, official notification by a competent judicial authority (notice and take down):** this option ensures the actual knowledge and provide legal certainty for intermediaries.
2. **Simple notification determining actual knowledge:** several shortcomings can be easily identified with the fact that the notice could come from official as well as unofficial sources; the burden of proving the illegality would stay with the provider (i.e. obvious crime vs complex query); the risk of such a system is to have the notice and take down applied consistently by the intermediary on all notifications and without proper legal assessment in order to escape liability. As mentioned above, it is of key importance to clarify and define minimum requirements as to when a provider has “actual knowledge” to reduce legal uncertainties for all parties involved. The UK law has laid down requirements similar to those listed under Question 53.
3. **Statutory requirements:** some countries do not provide a formal or simple notification procedure but set specific requirements to be observed by courts (i.e. location of the information, nature, contact details of the sender, etc.).

**57. Do practices other than notice and take down appear to be more effective? ("notice and stay down", "notice and notice", etc)**

EuroISPA believes that the establishment of notice and stay down or notice and notice procedures should be evaluated comprehensively. We have reservations that the establishment of these procedures will have additional value. In principle, disputes should be solved directly between the parties concerned. ISPs, in their role of intermediaries, are an uninvolved third party. EuroISPA questions the practicability of these procedures that could lead to legal uncertainty and impose obligations that will undermine the established liability regime. Moreover, it must be safeguarded and ensured that ISPs, in their role of intermediaries, do not become judges of the illegality of content.

**Notice and notice**

EuroISPA believes that an additional notification procedure maybe an option that could resolve disputes amicably and put the liability where it should lie, i.e. in the hands of parties disagreeing on the legality of a given piece of content. Such a system could come into consideration exclusively for hosting providers and limited to the forwarding of a notification. Privacy laws and the secrecy of telecommunications should be respected, and fundamental freedoms must be strictly adhered to.

Furthermore, it has to be taken into account that any notification procedure, like the notice and notice, is based on the general assumption that:

- intermediaries are exempted from liability;
- the general no-monitoring obligation is preserved;
- a penalty against a claimant that files a wrongful notice is introduced.

### **Notice and stay down**

EuroISPA believes that such a system raises legal uncertainty, turns ISP in judges of the illegality of the content and imposes ongoing filtering or monitoring on users' communications while completely by-passing the judge intervention. As explained in the answers to questions 58 and 59, such filtering or monitoring methods are not only costly to implement and present a risk for users' fundamental rights, but they also have no proven effectiveness.

In practice, "notice and stay down" is incompatible with the principle in Article 15, "no duty to monitor" as in order to discharge a requirement that certain material stay down a hosting provider would have to constantly monitor their service for the reappearance of the notified material. Moreover, unless the notification was extremely narrowly construed to refer to exact digital copies of the same file, notice and stay down would be impossible to implement (for example, a notice demanding the removal and continued suppression of libelous content could not be considered to cover a repetition of the same libelous assertion in different words).

### **58. Are you aware of cases where national authorities or legal bodies have imposed general monitoring or filtering obligations?**

In principle EuroISPA Members report endeavors/attempts to oblige intermediaries to filter or monitor in different areas: gambling, copyright infringements, hate speech, etc. This attempts are not in accordance with the fundamental principles laid down in Article 15.

Concerning specific cases in Member States:

- In **Italy** a very ample filtering is carried out on a vast number of services as a result of general call barring (Decision 600/09/CONS of AGCOM) which automatically prevents every fixed line (unless the user opts-in) from access to value added services provided through the telephone network. Such services include several information society services.
- In **Finland** there is a law which grants ISPs' the right to filter/ block access to sites which are maintained outside Finland and contain child pornographic material. The list of sites is run by the Finnish police.
- In **Belgium**, in the case of SABAM v Scarlet, the court ordered the ISP to filter peer-to-peer Internet traffic, which requires monitoring all peer-to-peer traffic, and inspecting it to see if any particular file being transferred matches a file that has been notified by SABAM as owned by a copyright holder. This case is pending appeal.

**59. From a technical and technological point of view, are you aware of effective specific filtering methods? Do you think that it is possible to establish specific filtering?**

The discussions on filtering should in no case be limited to technical feasibility and the preliminary question one may expect from the European Commission is whether it is desirable, in line with Europe's values and economic interest, to even consider filtering methods. Such methods are difficult to be efficiently implemented in a resilient environment like the Internet that was designed to avoid barriers and blocks and find alternative ways to deliver information. This is particularly true in situations where the telecommunications providers' role is only a "mere conduit" of real-time transmissions, for example in peer-to-peer networks. The impracticability of such measures is grounded on several reasons:

- **Form a technological point of view:** an effective filtering is not possible. Easy to circumvent, all content is affected (particularly legal content). There are an impact and adverse effects on the network resilience, security and efficiency of the infrastructure. All content has to be transported/checked by a centralized filtering infrastructure in the ISP network. The risk is high for a general monitoring of content/users to have collateral damages such as hypothesis of over-blocking.
- **From a broader perspective:**
  - they bring with obvious implications with regard to the violation of fundamental freedoms;
  - not for-profit providers cannot be expected to put in place filtering technologies;
  - the needed economic investments in infrastructures and personnel are burdensome for providers and would significantly and durably impact the development of the European Information Society in a negative way. It also exists a risk of "mission creep", i.e. start addressing a specific issue and then enlarge the monitoring to other issues as well;
  - it exists a risk of "technology creep", i.e. the need to constantly up-to-date the filter in accordance to the technological evolution of the Internet communications (ex: encryption). Filtering leads to the development of encrypted protocols and never ending investments to catch up with illegitimate uses and services (as oppose to deal with the problem at its source), resulting in costly and ineffective measures.

Additionally, if an Internet access provider has to actively roll out a filtering technology with regard to (part of) the data transmitted on its network, it could be argued that it would have the unintended consequence of neutralising the application of Article 12 of the Directive which exempts the access provider from any liability regarding the information transmitted via its network on condition that it does not select or modify the information contained in the transmission. However, if one considers that filters do not imply the selection of the information contained in the transmission as they consist of "mere technical instruments", then the liability exemption would be lifted with the consequence that the provider risks to be held liable for the malfunctioning of the filtering technology on its network causing, for instance, illegal content not being intercepted. In other words, the ISP characterization as "mere conduit" could be jeopardized with serious consequences for the provider, its customers and the respect of Fundamental Rights.

As established in the context of the Belgian Scarlet-SABAM case, where the technical solution “Audible Magic” was proposed as a possible filter for peer-to-peer traffic, the Belgian court acknowledged that it well might not be effective or scalable. Indeed, it seems impossible that a technology could make a waterproof distinction on the basis of the legal/illegal nature of the communication or even the identification of what is in a file. Indeed, this depends on specific considerations not directly related to the filter technology but, for instance, to the authorisation or concrete license terms granted by the author or the collecting society and on the possible interference of statutory exceptions to copyright.

**60. Do you think that the introduction of technical standards for filtering would make a useful contribution to combating counterfeiting and piracy, or could it, on the contrary make matters worse?**

In the digital age the widespread of technologies have offered new opportunities for the online distribution of copyright protected content. While innovative business models meeting users’ needs and expectations, and allowing to best value copyright online,<sup>i</sup> have been slow developing, the content industry is calling for even more technical and regulatory solutions to address the issue of online copyright infringement.

To combat such phenomenon a variety of technical options, known as digital rights managements systems, have been developed and introduced in the operating system, program software, or hardware of a device such as copy control; file access control; restrictions on altering, sharing, saving, or printing; encrypting files for use only by authorized users; electronic watermarking, flagging, or tagging to signal to a device that the media is copy-protected. In addition, the content industry calls for the use of special “filters” by ISPs that would enable them to screen their broadband traffic with the purpose to identify content and files allegedly infringing their rights.

EuroISPA is concerned that the adoption of filtering technologies, while ineffective to better value copyright online, will bring with serious threats to privacy, innovation and creativity undermining software development and other technical innovations in this area, and imposition solutions that do not work for all stakeholders. The costs of filtering technology for network traffic will be a burden to the provider that would implement it and to its customers and consumers, and prove inefficient in the medium/long term as the technical progress risks to make such solutions obsolete.

EuroISPA does not believe there is an effective and proportionate way to apply ubiquitous content filtering measures to prevent online copyright infringements. The real question facing policy makers and industry is whether existing filtering measures are a proportionate, cost-effective, efficient approach to deal with online copyright infringements in a way which will not have considerable unintended consequences outside the scope of the problem being addressed.

In general, EuroISPA considers that the development of innovative content services that meet consumer expectations and needs is the most effective way to prevent online copyright infringement and is far more effective than measures aimed at restricting the rights of users to access online information. In this context, technologies meant to protect copyright-

protected content, developed on a voluntary basis with the necessary collaboration of rightsholders and with the objective of favoring online availability of content can, in certain cases, be used to foster innovative content services and business models. This type of collaboration can only be developed on a voluntary basis, in the context of the legal framework defined by the ECD. EuroISPA believes that the implementation of filtering measures at the level of communication networks will have the opposite impact.

Further we will assess the following requirements:

- the proportionality of the technological measure;
- the cost effectiveness and efficiency;
- the unintended consequences.

### **Proportionality**

As mentioned, there is considerable doubt as to whether existing network filtering technologies would be effective in achieving their stated goal, particularly as users can be expected to use relatively simple encryption techniques to remain “one step ahead” of the technology. Encryption of peer-to-peer traffic is already happening at an increasing rate; filtering measures are likely to serve only to encourage universal adoption of encryption to avoid detection. At the same time, filtering can be expected to result in a risk of degradation of network services, of user experience and in the inadvertent blocking of access to legitimate content. Additionally, the increased costs such technology bring with would contribute creating a further barrier to address the digital divide.

As detailed in the WIPO Conventions and the Copyright in the Information Society Directive (2001/29/EC), exemptions to copyright for legitimate, agreed purposes are recognised and uncontroversial parts of intellectual property legislation. It is entirely possible for users to wish to exchange files which do not breach copyright but which, nonetheless, would risk being “filtered” by network filtering technologies that only allow “approved” files to get through. Both the EU and Council of Europe have had a global leadership position for many years in promoting free speech and access to information. There is simply no existing filtering technology that would allow full use of current technologies while ensuring that legitimate users’ behaviours are not restricted.

As the costs of Internet providers would be increased if every user’s data needs to be filtered, these costs would ultimately be borne by consumers – including the huge majority of users who do not infringe copyright. It is difficult to imagine another scenario where innocent consumers are asked to pay to have their own legitimate use of a service monitored, in order to protect the interests of third parties with whom they have no relationships.

### **Cost effectiveness and efficiency**

Large-scale filtering of Internet traffic of a very big number of Internet users could cause a problem of costs, implementation and maintenance. Taking account of the evolution of ISPs architecture, such filtering assumes the implementation of a significant amount of equipment in the network, administration of this equipment and probably of the evolution of the network architecture itself.

EuroISPA, therefore, wonders:

- To what extent can it be considered proportionate or even desirable at any level that intermediaries, which do not benefit in any way from the alleged illegal activity, should finance, or be obliged to finance, a system of this scale?
- How much less acceptable does this approach seem when we consider that there is widespread agreement that these technologies offer no answer, or expectation of an answer, to the issue of encrypted files, meaning that an ISP investing heavily in such technology would see the investment rendered meaningless in a short space of time?

### **Unintended consequences**

On a wider scale, imposing filtering in a way which is likely either to result in legal content being made inaccessible or results in cross-border effects (where legal material becomes unavailable because it is illegal in another country, for example) has international legal implications. The UN Covenant on Civil and Political Rights (Article 19) states that *“everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice”*. A similar provision also appears in the European Convention on Human Rights.

### **62. What is your experience with the liability regimes for hyperlinks in the Member States?**

AND

### **63. What is your experience of the liability regimes for search engines in the Member States?**

Hyperlinks are central to the functioning of the Internet and can take various forms (the actual URL of a website, a short version of it, or an image linking to text, image or audiovisual content). Internet services as well as users are making use of hyperlinks to point at specific information hosted online. Individual users are increasingly making use of hyperlinks on social network services, to point at specific information or piece of content. Various courts around the EU have recognised the crucial role of search engine in helping users to find their way through the growing amount of information available online, providing them with hyperlinks to the relevant information.

However, different interpretations around Europe have led to the application of different ISP liability limitation regime for hyperlinks and search engines. As for search engines, they are expressly covered under provisions similar to “mere conduit” in national implementing legislation in Austria, Bulgaria and Liechtenstein. In Hungary, Portugal, Romania and Spain, they are expressly covered under provisions similar to “hosting” in national implementing legislation. Hyperlinks are expressly covered under provisions similar to “hosting” in national implementing legislation in Austria, Liechtenstein, Portugal, Romania and Spain.

In Italy there is no precedent yet as to ISP liability for hyperlinks (e.g., to web-sites where programs for sharing contents may be unloaded), although in the course of an interim relief procedure started by FAPAV and SIAE this was (unsuccessfully) used as an argument to invoke Telecom Italia liability towards the companies represented by FAPAV whose contents were allegedly shared by Telecom Italia Internet service users. However, the Court

(Tribunal of Rome, FAPV vs. Telecom Italia, order no. 415 of 2010) did not find any liability, as the outcome of the interim procedure. On the other side, a liability of search engine was found by the same Court in another case (Tribunal of Rome, 16 December 2009, R.T.I. S.p.A. vs. You Tube Inc. + Google UK ltd).

In order to create the conditions of innovative information services to develop across Europe, it is crucial to provide some guidance on the ISP liability regimes that may apply to different services. There is a need to confirm that providers of hyperlinks as well as search engines fall within the definition of information society services. If express national legislation exists, they should be applied, and in the absence of such provisions, the provider of links may be covered under Article 12 and/or 14. As for search engines in the absence of express national legislation the Commission should issue guidance that search engines should be considered under provisions related to mere conduit (Article 12) and that any national legislation should follow this approach.

**64. Are you aware of specific problems with the application of the liability regime for Web 2.0 and "cloud computing"?**

EuroISPA did not witness any specific problem on this regard.

**65. Are you aware of specific fields in which obstacles to electronic commerce are particularly manifest? Do you think that apart from Articles 12 to 15, which clarify the position of intermediaries, the many different legal regimes governing liability make the application of complex business models uncertain?**

Intermediaries wishing to develop services and new business models face licensing, levy problems of copyright laws. Innovation is at stake, since the cost of managing legal uncertainty is such that it acts as an obstacle to innovation.

We would also mention contractual inequality between suppliers and retailers as an obstacle to e-commerce. This is something identified by the Commission's 2009 Report and Communication on cross-border e-commerce. Small-medium enterprises' retailers often find themselves in a weaker negotiating position vis-à-vis their suppliers. The result is sometimes that they are contractually or in practice restricted from making full use of the Internet, for example from selling online across borders, making use of online platforms or setting up an online-only operation. This situation was also identified by the recent Parliamentary report on "Completing the Internal Market for e-Commerce", holding that:

*"... online platforms have played an important role in boosting (especially cross-border) e-commerce in Europe, enabling market access by hundreds of thousands of SMEs, and offering consumers greater choice whilst introducing many examples of good practice for boosting trust and transparent information about rights and obligations and facilitating the resolution of disputes between parties to an online transaction, where necessary; "*

*“...existing vertical distribution agreements are often used to avoid or restrict online sales, thus denying retailers access to wider markets, undermining consumers' rights to a wider choice and better prices, and thus creating barriers to the expansion of commerce”.*

**66. The Court of Justice of the European Union recently delivered an important judgment on the responsibility of intermediary service providers in the Google vs. LVMH case. Do you think that the concept of a "merely technical, automatic and passive nature" of information transmission by search engines or on-line platforms is sufficiently clear to be interpreted in a homogeneous way?**

The ECJ has made clear in the Google vs. LVMH case that the hosting status is not affected by the fact that the service provider sets the payment terms of its services, provides general information to its service recipients, processes the data entered by the recipients or controls the final display of data (e.g. in the form of ads).

When referring to Recital 42, i.e. a non operative part of the ECD to define requirements for the application of the liability limitation of Article 14, the ECJ ruled that:

*113: “... In that regard, it follows from recital 42 in the preamble to Directive 2000/31 that the exemptions from liability established in that directive cover only cases in which the activity of the information society service provider is ‘of a mere technical, automatic and passive nature’, which implies that that service provider ‘has neither knowledge of nor control over the information which is transmitted or stored’.”*

Unfortunately, the ECJ wrongly assumes that Recital 42 applies also to hosting services. It is clear from the text of Recital 42 that it is concerned with mere conduit and caching services (Articles 12 and 13). The only conditions relevant for determining responsibility of a hosting service provider are that: (i) the service provider has actual knowledge of the illegal activity or information and (ii) the service recipient is acting under the authority or control of the service provider.

If these conditions do not exist, the service provider cannot be held liable for the data stored at the request of a client, unless, having obtained knowledge of the illegal nature of these data or of that client's illegal activities, it failed to act expeditiously to remove or to disable access to the data concerned. If Recital 42 would cover hosting, it would constrain and limit the liability exemption laid down in Article 14.

In any case, guidance are required to make clear that voluntary systems to address acts or contents potentially illegal or infringing terms of uses of services, should in no case be construed as calling into question the mere technical, automatic or passive role of the service provider.

As pointed out in answer to question 53, it is crucial to make sure that voluntary efforts from ISPs to ensure that no illegal content is stored or transmitted require a level of activity by the intermediary. Even if encouraged by the Directive (e.g. Recital 40), they can in no case be

interpreted as providing a basis for deciding that the intermediary is active, has knowledge of or control over the data stored and is no longer neutral, passive, automatic and merely technical, so denying the benefit of the liability limitation regime. Failing to do so will act as a disincentive for ISPs to act voluntarily and encourage a hands-off approach.

**67. Do you think that the prohibition to impose a general obligation to monitor is challenged by the obligations placed by administrative or legal authorities to service providers, with the aim of preventing law infringements? If yes, why?**

The prohibition to impose a general obligation to monitor is challenged by administrative or legal authorities whose increasing obligations on ISPs could lead to a factual monitoring, so undermining and steadily eroding this fundamental principle of the Directive.

The general obligation under Article 15 ECD proved to be sufficiently flexible and well-drafted as to allow public authorities to put additional obligations on ISPs. Indeed, if the “general” monitoring obligation is forbidden, Member States are not prevented from imposing “specific, limited and clear” obligations on ISPs for individual cases. This interpretation is confirmed by Recital 47 which adds that courts can still request an ISP, even if not liable for the infringement, to terminate or prevent it through injunctions. However, when imposing specific obligations, a public authority should carefully assess the scope of it to avoid that the measure produces effects equivalent to a generalised monitoring.

For further considerations, see points 52, 58, 59 and 60.

**68. Do you think that the classification of technical activities in the information society, such as "hosting", "mere conduit" or "caching" is comprehensible, clear and consistent between Member States? Are you aware of cases where authorities or stakeholders would categorise differently the same technical activity of an information society service?**

The classification is based on the technical activity and service offered by a provider, and allows for a flexible and differentiated assessment. Concerning Article 14, it specifies that a provider can benefit from the liability exemption if it does not create the content but limit its service to the storage of the information (“consists of”). Problems arise with complex services, such as auction platforms or cloud computing, where the storage is only a single component of the service provided. To what extent the fact to provide “also” a hosting service can allow a provider to be covered by Article 14? These typically have been dealt with on a case-by-case basis, depending on the “non-hosting” activities in which the service is engaged. National courts reached different conclusions, though lately we have seen a trend towards a greater understanding of the multiple role intermediaries have and recognition that merely because an intermediary engages in non-hosting activities as well, it is not excluded from the scope of Article 14.

**69. Do you think that a lack of investment in law enforcement with regard to the Internet is one reason for the counterfeiting and piracy problem? Please detail your answer.**

EuroISPA believes that law enforcement agencies already have the required powers to address problems related to counterfeiting and piracy. The problem lies with the content providers and the need for them to develop new appealing business models that are currently lacking in the market. We continue to experience a change of the economy with the transformation of existing markets, the evolution of existing business models and the development of channels of distribution for the digital age. Enforcement agencies must focus on the development and encouragement of adequate and attractive new business models, with recourse to legislation based on sustainable principles. The development of legal markets promoting and supporting digital content will constitute one element of success in addressing online copyright infringements to the benefit of the creative industries, consumers and all stakeholders of the online environment. The EU could assist the creative industries in shifting towards more sustainable business models by moving its regulatory focus away from enforcement, restrictions and sanctions and towards measures that promote the establishment of innovative services. Furthermore, EuroISPA considers that ISPs under any circumstances should be burden with a monitoring and enforcement role. Fundamental Rights of information, privacy and communication are severely undermined when ISPs, in practice, become prosecutors.

***EuroISPA** is the world's largest association of Internet Services Providers (ISPs) representing the interests of more than 1800 ISPs across the EU and the EFTA countries. EuroISPA is a major voice of the Internet industry on information society subjects such as cybercrime, data protection, e-commerce regulation, EU telecommunications law and safe use of the Internet ([www.euroispa.org](http://www.euroispa.org)). Contact: Andrea D'Incecco, Head of Policy (+32 2 503.22.65/ [andrea@euroispa.org](mailto:andrea@euroispa.org)).*