ID: Telef05162

## GENERAL COMMENTS

Telefónica is a strong supporter of the Commission's efforts to increase the use of ecommerce across the Union. Electronic communications providers are significant enablers of ecommerce, responsible for important investment in next generation infrastructures which lie behind any ecommerce activity.

Telefónica acknowledges that there are still many obstacles to overcome if ecommerce is to grow, but finds that these lie outside the specific legal framework as set out in the eCommerce Directive, which finds a good balance between the needs of businesses, intermediaries and consumers.

We would recommend that the EU focus its efforts on more pressing obstacles to electronic commerce, such as:
- reforming the online content licensing regime and creating a true Digital Single Market;
- facilitating innovative payments mechanisms, which could help to foster new business models for content creators;
- helping to create trust for citizens online through revised data protection rules which offer a consistent and confident experience when using electronic communications services;
- setting clear rules to encourage investment in the next generation of networks, through which new services can be delivered, and more of Europe's citizens connected;
- harmonising consumer protection rules so that it is easier for SMEs to offer their products and services with confidence across the Single Market.

The Digital Agenda covers many of these points, and Telefónica urges the Commission to maintain the above issues as priorities therein. Regarding the question on the eCommerce Directive, Telefónica thinks that, in general, the Directive strikes the right balance between legal certainty at EU level and flexibility for member states to translate the Directive into internal legislation in line with their legal traditions and case law. No significant problems have arisen which appear to call for reform, particularly in the core issue of the liability regime.

Therefore, Telefónica will provide answers for some, not all, the questions of the questionnaire.

### Issue 2: Questions concerning derogations from Article 3(Article 3(4) and Annex)

*The Electronic Commerce Directive includes in its Article 3 a so-called "internal market clause", with case by case derogations provided for Article 3 (4). This clause allows information society service providers to offer cross-border services whilst remaining subject to the legislation of their Member State establishment. Member States may, under certain conditions, impose case by case derogations to this principle to ensure the protection of certain conditions, impose case by case derogations to this principles to ensure the protection of certain interests such as public order, public health, public safety or consumer protection. Any such derogations must be necessary and proportionate to the objective pursued. They must be adopted within the framework of an administrative cooperation mechanism between Member States and notified beforehand to the European Commission.*

*Moreover, the Annex to the Directive provides for exemptions from Article 3, in particular for contractual obligations relating to contracts concluded with consumers. Since 2000, the UE´s legislative framework has evolved, in particular Community legislation having as an objective consumer protection (in particular the application of the directives on distance contracts and on the sale and guarantees of consumer goods; the adoption of the Directive on the unfair commercial practices1 and the proposal for a Directive on consumer rights in 2008), and with the Directive on services on the Internal Market2, which was due to be transposed by the end of 2009. Article 20 of the Services Directive is likely to have a direct impact on the issue of cross-border sales to consumers as its paragraph 2 prohibit the application of discriminatory provisions relating to the nationality or place of residence of the recipient of a retail service. Differences of treatment are allowed only if such service providers can demonstrate that they are justified directly by objective criteria.*

**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?**

The current system of reporting, paying and refunding copyright royalties hinders rather than encourages cross border business.

For example, the European Commission´s decision on the CISAC case[3] tried to put an end to certain practices developed by the European collecting societies regarding online music distribution, as such practices were restricting competition within the European market. The European Commission´s purpose was to make the collecting societies compete by means of a pan-European license throughout Europe, restricting them to operate as territorial monopolies.

---

[1] 2005/29/CE, OJL 149 of 11.6.2005, p. 22-39.
[2] 2006/123/CE, L 376 of 27.12.2006, p. 36-68.
[3] Case COMP/38698- CISAC Commission Decision of 16th July 2008.

However, the movements of certain collecting societies and some major music publishers -after the European Commission's decision- far from clarifying and making it more straightforward to operate, have added more complexity and lack of transparency, and have put up new obstacles regarding multi-repertoire and multi-territory licenses, territorial pricing differences and led to legal/commercial uncertainty in order to ascertain which entity is entitled to licence, which must be faced by cross border commercial users.

For these reasons, the process of clearance of the copyrights for online music distribution is getting more difficult for multinational commercial users. Before the CISAC decision it was enough to get from each of the collecting societies in each country the total clearance of all the repertoires. After the CISAC decision, some music authors' publishers decided to withdraw their catalogues from national collecting societies and to choose an exclusive representative at a European level (one specific collecting society or an association of them). This has had the effect of replacing the previous territorial monopolies with new monopolies based on repertoire. Another problem is that the supposed new Pan-European licensing scenario -following those initiatives- is not workable as the national legislative situations are different and, in some cases, do not allow those associations to licence all the rights associated to a creative work (e.g. public performance, mechanical, making available, etc). Therefore, in that scenario the commercial users trying to exploit the rights in a cross-border basis would need to obtain the clearance from each of the national collecting societies where it operates and also from each of those new entities representing certain catalogues and, furthermore, to face the uncertainty, lack of transparency, complexity and administrative problems that such a new system generates.

In the current landscape, multinational commercial users must to face several problems that impede or difficult cross-border trade:

- from a monopoly based on territory we are moving to monopolies based on repertoires, which could be even more dangerous for the Pan-European licensing regime.
- the Pan-European licence is proving not workable as in some countries there is no way of licensing all the rights involved on a Pan-European basis.
- there is no competition on prices; the offered prices continue to be prices of the country of origin; there are no Pan-European prices.
- the increasing costs of administration due to the maintenance of different reporting and payment systems.
- the uncertainty that double payments might be made.
- instead of tending towards a one-stop-shop system we are going to a system of fragmented repertoires and multiple points of contact.

Consequently, a solution to that problem must be sought in order to reinforce the regulatory framework and to grant an adequate level of security that avoids cross-border users being unintentionally unlicensed or having to assume the risks mentioned before, such as double

payments, uncertainty regarding the rights licensed and lack of competition among the different collecting societies. In that sense, we think that it is necessary to work on two aspects:

- the harmonisation of IP legislation across the member states, in order to facilitate the creation of a Pan-European licence
- the creation of effective competition among collecting societies, and avoiding any anticompetitive agreement between them, for example, on the prices they apply or on potential sharing of information regarding the reporting and payment systems.

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

The differing copyright levies that apply in different territories to particular devices for the purpose of licensing private copies do not encourage a simple and universal regime across Europe.

Article 5.2 b) of Directive 2001/29/EC entitles Member States "to provide exceptions or limitations to the reproduction right (...) in respect to reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial, on condition that the right holders receive fair compensation (...)".

In that regard, the fact that each member state has the power to regulate such "fair compensation" in a different way, based on territorial rights, makes cross border management of copyright levies an impediment to ecommerce since the current system brings cross-border commercial users to a scenario in which they may pay and report copyright levies in several countries for the same goods or discriminate between traders on the basis of nationality.

For that reason, we find it important to seek solutions for the sake of equality and competitiveness in the EU economy.

**Issue 3: Cross-border commercial communications, in particular for the regulated professions.**

*Articles 6 and 7 of the Directive cover commercial communications and, in particular, unsolicited commercial communications.*

**38.- Are you aware of any mechanisms in your Member State which guarantee that unsolicited commercial communications can be identified in a clear and unambiguous manner by addressee?**

Yes.

UK Regulations do not prescribe how to meet the requirement for information about commercial communications to be “clearly identifiable”. UK Government guidance at the time of implementing the Directive explains the requirement could be achieved either through a header, before the communication is opened, or in the body of the communication itself.

In the case of Spain, the advertising companies are subject to a strict control by the Spanish regulator in relation to the need to clearly identify, in each communication (whatever electronic means are used, email, SMS or MMS), the natural or legal person on whose behalf the commercial communication is made and also if the communication is for simple information or for advertising purposes.

It is clear that if the sender of a communication is clearly identified the recipient can easily check:

- If the communications is just for information purposes and if the sender of the communication has a prior contractual relationship with him which entitles him to do it.
- If the communication has a commercial nature or not and if the sender holds the right authorization to proceed with these commercial communications.

**39.- Do measures exist in your Member State which guarantee that the service provider who sends unsolicited commercial communications by email regularly consults "opt-out"registers ( in which natural persons who do not wish to receive this type of communication can register)? If so, are these registers respected?**

The Directive says that businesses must consult regularly and respect opt-out registers before sending unsolicited commercial communications. The UK decided to omit this provision when implementing the Directive. The Government at the time considered that industry self-regulation and codes of conduct already gave effective protection to the recipients of spam and, furthermore, that Unsolicited Commercial Communications by email would be subject to the rules imposed by the Privacy and Electronic Communications Directive 2002/58/EC.

Accordingly, The UK's main law for dealing with spam is the Privacy and Electronic Communications Regulations 2003, which implemented the EU Directive. It requires businesses generally to have prior consent before sending unsolicited commercial email to "individual subscribers" (with a “soft opt-in” option).

In Spain, all enterprises, institutions, agencies and advertisers that conduct publicity campaigns by e-mail should consult opt-out registers ("Robinson List") in which natural persons not wishing to receive such commercial communications can register themselves. This advertising exclusion file ("Robinson List") can also avoid receiving unsolicited commercial communications from companies whether or not there is a prior commercial relation with them.
In addition, this register also allows interested parties to decide through which other means (such as voice telephone, SMS, MMS) they agree with to receive commercial communications even with companies with whom they have no maintained any contractual relationship.

**40.- Is the legislation of your Member State sufficiently clear on the criteria making it possible to determine if a commercial communication can be regarded as unsolicited or not?**

Neither the eCommerce Directive nor the Privacy and Electronic Communications Regulations define "unsolicited". However, the UK Information Commissioner's guidance notes provide some explanation.

In Spain, the criteria are clear enough to determine if a commercial communication can be regarded as unsolicited or not.

**41.- Is the " acquis communautaire" (Europena Law ) on unsolicited commercial communications and national regulations well-adapted to new forms of commercial communications?**

Yes. In our opinion the European legislation on unsolicited commercial communications clearly covers new forms of commercial communications (e.g. social networks amongst others).

**Issue 5: *Interpretation* of the provisions concerning intermediary liability in the Directive**

*The Electronic Commerce Directive was drawn up and negotiated in the late 1990s with the aim of developing a balanced framework for Internet intermediaries that on the one hand protects stakeholders' rights and on the other encourages the development of new information society services. One essential piece of this framework is the way in which intermediary liability was established, defining the conditions for exemptions of liability of intermediary Internet service providers for certain activities: "mere conduit", "caching" and "hosting" (Articles 12 to 14). These mention the concepts of "actual knowledge" of an*

*infringement and of an "expeditious" response. The Commission, and also national courts and administrations, have frequently been called on to interpret these concepts. There have not been particular problems in applying these concepts to real situations.*
*Article 14(1)(b) leaves open the possibility of notice and take down procedures to be agreed between parties, if problematic information is detected. The Directive does not regulate the detail of such procedures.*

*Article 15 states that providers offering the services covered by the Articles above have no general obligation to monitor but that Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities.*
*The Commission has found, through its contacts with the various stakeholders, that the interpretation of the provisions concerning the liability of intermediaries is frequently considered necessary towards solving problems. The study commissioned on this issue (see above) found differences in interpretation between national courts and even within Member States.*

***GENERAL COMMENTS***

The principles around intermediary liability contained in the Directive and the lack of either obligation or legal capacity to monitor internet content have provided important guidance to ICT companies like Telefónica. They set out clear rules for companies who provide consumers with access to ICT services, combining efforts and resources to achieve the strong growth of internet over the last ten years. Under the no monitoring principle, users were assured that their private communications were protected, thus generating confidence in using electronic communications. On the other hand, ISPs have been willing to create the possibilities of unhindered internet connections because they were not held liable for the content of the communications sent over those connections. In Telefónica's opinion the current eCommerce Directive strikes the right balance between the obligations regarding the protection of right holders (intellectual property rights is a good example of this) and the need to preserve at the same time Internet access freedom, confidentiality of communications, personal data protection and privacy on line.

Any step taken in the way of ignoring, eroding or weakening the principle of liability protections of intermediaryies will seriously compromise citizens' confidence when online.

Concepts like "actual knowledge", "mere conduit" or "hosting" are defined in articles 12 to 14 of the Directive in general and harmonized terms, thus letting national legislation to go into more factual and specific definitions. Although there have not been serious problems so far, the increasing claims by copyright holders considering as "actual knowledge" any private notice of unlawful materials, even without giving the client or user the opportunity to counter the claim is threatening to undermine the whole balance of the legislation.

Fundamental rights, like the right to due process and the privacy of personal data, could be seriously threatened if the Directive is amended to introduce any obligation on intermediaries to act only on the request of private agents or to impose notice and take down procedures.

In Telefónica's opinion, the current wording of the eCommerce Directive is and continues to be enough to deal with the question of liabilities, allowing national regulation to deal with the detail which best accommodates European law, fundamental rights and national legal structures. From the experience in the law and court practices in the countries in which Telefónica runs its operations, no serious problems have arisen in the interpretations of these concepts.

Regarding the issue of intellectual property rights and ecommerce, Telefónica is fully aware of how important the protection of copyright is to encourage the creativity and the development of powerful content for online use and trade. While Telefónica is fully engaged in this goal, we firmly believe that punitive approaches will not provide any positive outcomes if they do not go hand in hand with other actions: to remove obstacles and competition problems in the current copyright management system, to allow new business models to happen and to promote information and educational campaigns to foster the cross-border trade of content in digital environments. To achieve that, rightsholders should co-operate with others agents in the value chain in offering innovative and interesting legal ways to access their contents. Electronic communications operators, information services providers and rightsholders are and should remain in a position to develop agreements on a bilateral basis as part of commercial negotiations.

**52. Overall, have you had any difficulties with the interpretation of the provisions on the liability of the intermediary service providers? If so, which?** ***BUS (ISPs), PUB SERV, INFOSOC LAW PUBLIC SERVICE***

No specifically.

As we all know Article 15 stresses that a duty to monitor may not be imposed upon online intermediaries. Despite this strong and clear statement, surprisingly, recital 48 establishes that Member States may impose upon intermediaries a "duty of care, which can reasonably be expected from them and which is specified by national law, in order to detect and prevent certain types of illegal activities". Thus, Article 15.1 prohibits the imposition of an obligation to monitor, while recital 48 at the same time permits a duty to detect unlawful material.

From Telefónica's experience, these obligations to detect and prevent illegal activities have not been imposed by regulations, but implemented by self-regulatory tools by intermediaries focusing only on a limited range of criminal behaviour, like child abuse.

Experience has shown that self regulation has been the better way of striking the right balance between Article 15 (no monitoring principle), and recital 48. Telefónica believes that

any amendment of the Directive should withdraw any possible regulation imposing specific obligations to detect or prevent hypothetical or future illegal activities.

Telefónica strongly disagrees with the claim of copyright rightsholders to introduce obligations to monitor, detect or prevent unlawful activities, as important fundamental rights like the right of due process, freedom of expression and privacy and data protection could be at risk if this obligation is imposed without a prior court order.

**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? *BUS (ISPs), PUB SERV, INFOSOC LAW PUBLIC SERVICE***

No specific problems have occurred, although national implementation and court practice differ between member states considerably when assessing "actual knowledge". Some member states require a formal procedure and an official notification by authorities in order to assume actual knowledge of a provider, whilst others leave it to courts to determine when actual knowledge exists after having assessed the factual circumstances.

Any regulatory change which consisted of considering that actual knowledge exists when a private notice from a private party like copyright holders addressed to a user of information society services without a court order, will risk obliging the intermediaries to act against behaviours that could in the end not be declared as unlawful by the court. As important fundamental rights are involved, extending in this way the concept of "actual knowledge" would not be proportionate.

**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? *BUS(ISPs), PUB SERV, INFOSOC LAW PUBLIC SERVICE***

No special problems have arisen.

**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? *BUS (ISPs), PUB SERV, PRIV***
We refer to questions 52 and 53.

Article 14 leaves Member States with the discretion to establish "notice and take down" procedures according with their internal legal systems. Clearly, there is an intention of some Member States to introduce such procedures as the following Member States have done:

*NATIONAL DEVELOPMENTS*

- *FR*: The Constitutional Council has approved the law on the criminal protection of intellectual property on the internet (so-called 'Hadopi 2 ) on October 28, 2009: It foresees that courts can order the disconnection of internet subscribers for up to one year after piracy acts have been recorded by the officers of Hadopi.) with only one minor change.

- *ES:* On January 8, 2010 the Council of Ministers adopted a draft bill that proposes the creation of an intellectual property commission that would be competent to interrupt an information society service or to withdraw content from websites when intellectual property rights (IPR) are infringed. The draft bill also specifies that the responsible authorities may require providers of information society services to provide the necessary data to identify the infringers of IPR. However, the prior authorization of a judge is necessary to execute the measures adopted by the administration when these measures could violate fundamental rights and freedoms.

- *UK*: In January 2010, the Minister for Digital Britain announced that ISPs will have to bear 75% of the costs related to the implementation of the graduated response and called for a quick adoption of Ofcom code of practice (approved by Ofcom or, if no industry code is put forward for approval, drafted by Ofcom) which would set-out in detail how ISPs must meet the obligations to:

    1. notify their subscribers if the internet protocol ('IP') addresses associated to them are reported by copyright owners as being used to infringe copyright; and,
    2. keep track of the number of reports received about each subscriber, and compile, on an anonymous basis, a list of some or all of those that have been reported on. After obtaining a court order to obtain personal details, copyright owners would be able to take action against the subscribers that are included in the list.

  ISPs have opposed the bill, claiming that it undermines the person's right to be presumed and treated as innocent and also on the grounds that it is placing on them an administrative burden and additional costs.

Telefónica rejects any proposals which involve suspension of a customer's connection for unlawful downloading without previous court orders, as it interferes with users' right to freedom of expression.

Only in cases of serious crimes like paedophilia, in which there is unquestionable evidence that a criminal offense exists, is there a case where action taken by intermediary could be a proportionate response when there is not a previous judicial decision.

**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? *BUS (ISPs), INFOSOC LAW PUBLIC SERVICE***

Telefónica O2 UK is a member of Internet Watch Foundatión4. This is generally recognised as a successful scheme to combat hosting of illegal child abuse images.
In relation with Telefónica's stance on notice and take down procedures, see responses to the previous questions on issue 5.

**57. Do practices other than notice and take down appear to be more effective? ("notice and stay down"[13], "notice and notice"[14], etc) *BUS (ISPs), INFOSOC LAW PUBLIC SERVICE***

Under this paradigm, Telefónica believes it is necessary to have a transparent and open dialogue, involving all the stakeholders, in order to make all the elements, of supply and demand of online contents, coincide. As explained before, the fight against unlawful online content requires a whole set of educational measures, removing competition constrains and new business models. A transparent and open dialogue, involving all the stakeholders, is essential in order to make all the elements of supply and demand of online contents to coincide.

**58. Are you aware of cases where national authorities or legal bodies have imposed general monitoring or filtering obligations? *BUS(ISPs), INFOSOC LAW PUBLIC SERVICE***

The UK Digital Economy Act (DEA) introduces a reserve power whereby (upon an assessment by Ofcom) the Secretary of State can require ISPs to impose require technical measures (such as bandwidth capping or temporary account suspension or indeed other technical measures to limit service) in the event the DEA initial obligations (sending warning notices and subsequent legal action against persistent infringers) do not prove as effective as expected. Ofcom points out that if the Government decides to do this, it would require further legislation, approved by the Parliament. It will also be for Government to set out in further legislation any criteria which will be used for the application of technical measures against a subscriber.

Telefónica believes that any measure to be adopted must observe the existing legal framework, and therefore any action to promote the access of lawful content on the Internet or to discourage the access of unlawful content should use the existing legal obligations, with

[4] http://www.iwf.org.uk/

due consideration of the Fundamental Rights of Citizens, as well as the general principles and rights of criminal law.

Trying to extend the European legal framework beyond the jurisprudence recognized by national courts and the European Court of Justice will only create legal uncertainty and popular rejection of any of initiatives adopted.

**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? *BUS (ISPs), INFOSOC LAW PUBLIC SERVICE***

Telefónica is not aware of any filtering methods that are effective in dealing with large scale infringements of the kind that we are often asked to deal with by rightsholders. Suggestions that filtering/ technical measures are the "answer" to combating illicit P2P piracy etc are unproven.

In general, any filtering technology is circumvented by users, based on the knowledge they possess by already using the internet and downloading technologies, or via more expert users who share their knowledge with others. Examples includes proxies to mask IP addresses, altering the content slightly in order to avoid detection, or using different forms of accessing or sharing content. The very structure of the Internet facilitates the exchange of information and the circumvention of blockages in the network, and so filtering of content which is desired by users is an extremely difficult challenge.

In UK and regarding P2P Piracy, in the course of the UK consultations on the DEA, it was noted that were technical measures (such as blocking/ filtering etc) to be introduced, in the absence of attractive legal alternatives to illicit P2P, there would still remain the incentive for those that wished to continue to share content illicitly via P2P (or via other mechanism) to circumvent whatever technical measures were introduced.

Accordingly, the UK Government at the time of the DEA made clear that a thorough examination of the proportionality and effectiveness of any technical measures would have to be undertaken before ISPs could be required to implement technical measures.

**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? *BUS(ISPs), INFOSOC LAW PUBLIC SERVICE***

As mentioned above, the effectiveness of general filters is questionable from a theoretical and a practical point of view. The introduction of technical standards may indeed make matters worse, as circumventing the standards in one filter would, if they were similar in all filters, work for all other filters. Indeed, in the UK debate over the implementation of the

Digital Economy Act, it was recognised by rightsholders that users could circumvent technical measures.

If technical measures were to be introduced (and as above the case for such measures has yet to be proven), then whilst widely supported technical standards can help deliver economies of scale and hence reduce implementation costs, there remains the fundamental issue as to the benefit such measures can deliver given the degree to which such measures can be circumvented or avoided by those engaged in counterfeiting and piracy. Furthermore, the question of "what" needs to be filtered needs to be addressed. In response to the UK Consultation on the DEA, many respondents proposed that a Court should determine "what" content should be subject to technical measures.

In addition, we would like to point out that another way to improve the protection of children online and to prevent illegal content propagation is raising awareness and education of children, teachers and parents.

**61. Are you aware of cooperation systems between interested parties for the resolution of disputes on liability?** ***BUS (ISPs), INFOSOC LAW PUB SERVICE***

Overall, Telefónica acts as an intermediary. As a general principle, the rules on electronic commerce states that intermediaries will not be held liable if legal requirements are met. We have not been involved on disputes regarding liability and consequently we have not gone to alternative dispute resolution systems.

**62. What is your experience with the liability regimes for hyperlinks in the Member States?** ***BUS (ISPs), INFOSOC LAW PUBLIC SERVICE***

**63. What is your experience of the liability regimes for search engines in the Member States?** ***BUS (ISPs), INFOSOC LAW PUBLIC SERVICE***

**64. Are you aware of specific problems with the application of the liability regime for Web 2.0 and "cloud computing"?** ***BUS (ISPs), INFOSOC LAW PUBLIC SERVICE***

Web 2.0 – the elements of the Internet which are more interactive and demand input from users – and cloud computing – when data is stored on remote servers rather than on one's own device – creates an interesting new set of circumstances to which the European legal framework applies, including the current rules about liability of intermediaries. It is premature to foresee if any problem could arise in the application of present rules contained in the eCommerce Directive that could not be better dealt with by self-regulation.

Should any specific rules be need in the future, this new regulation has to be proportionate and strike the right balance between the fundamental rights of all stakeholders and be focused on growing the possibilities for ecommerce.

**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? *BUS (ISPs), INFOSOC LAW PUBLIC SERVICE***

Although there could be differences between member states on how they transposed articles 12 to 15 into their national legislation, there have not been significant problems in its practical implementation.

Larger obstacles to ecommerce can be found in rules governing payments systems, content management and consumer rules. Currently it is difficult to access content online because of restrictive management of content, a lack of possibility for easy payment for the content (particularly for certain sectors of the population who do not have access to credit cards), differing rules for consumer protection which are defined in the country of residence of the consumer and the requirement of Data Protection rules that provide the necessary consumer confidence without prohibiting business models or being too bureaucratic (eg. transfer of data);

Other elements which can assist in growing the e-commerce market include sensible regulatory approaches to the Net Neutrality debate – not prohibiting new business models- or more generally speaking, a framework which fosters investment in the sector ( e.g. broadband investment).

**66. The Court of Justice of the European Union recently delivered an important judgement on the responsibility of intermediary service providers in the Google vs. LVMH case[15]. 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? *BUS (ISPs), INFOSOC***

**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? *BUS (ISPs), INFOSOC LAW PUBLIC SERVICE***

See answer to the previous questions*.*

**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? *BUS(ISPs), PUBLIC SERVICE INFOSOC LAW***

Telefónica is not aware of significant problems arising from different understandings of the hosting, mere conduit or caching concepts.

**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. *BUS (ISPs), INFOSOC LAW PUBLIC SERVICE***

Telefónica strongly disagrees with this simplistic approach to counterfeiting and piracy online. As explained before, the lack of sound offers of legal content, the lack of evolution of traditional business models, competition problems between right managements entities and the need to improve the education and awareness of the citizens about this important issue are the key factors to be dealt with in the short term. An approach based only on repressive measures will be not only ineffective but could even have counterproductive effects for the development of ecommerce. Customers and businesses should have confidence in using electronic communications to facilitate and improve their relationships, and not feel that they might be monitored by private entities working at the behest of rightsholders.

Brussels, 22nd October 2010