Introduction

European Digital Rights (EDRi) is an association of 29 digital civil rights associations from 18 countries.

Preliminary comment:

EDRi notes that the questionnaire, intended as a public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce (2000/31/EC), is proposed in the so-called "Interactive Policy Making" (IPM) framework, identifying "stakeholders" and directing specific sets of questions to some of them.

EDRi considers that European legislation and regulation matters to all and may impact far more citizens and society organs than those identified by the Commission concerning a given sector. As a matter of fact, EDRi fits into none of the "stakeholder" categories identified by the Commission: it is an association of digital civil rights national associations of citizens and is therefore fully and directly concerned by the provisions of the E-Commerce Directive.

Moreover, the questionnaire itself shows that emphasis is put on business and consumer aspects of information society services, despite the fact that EDRi would argue that fundamental rights and democracy issues are also – and primarily – at stake in the e-commerce Directive.

In addition, while EDRi understands that such questionnaire format will ease the workload of the Commission services, our association does not necessarily agree with the range and the kind of questions, the way in which they are phrased and the categories of responders to which they are directed. Therefore, in responding to the consultation, EDRi has taken the liberty to add considerations that are not considered by the Commission and to discard some of the questions. When relevant, reference to specific questions from the questionnaire is nevertheless provided.

Main issues with the E-Commerce Directive:

EDRi is very concerned about the future of the E-Commerce Directive because any lack of clarity or thoroughness for the safe harbours available to Internet intermediaries leads, almost

inevitably, to the undermining of fundamental rights guaranteed by the European Convention on Human Rights and the European Charter on Fundamental Rights.

Lack of legal certainty for intermediaries can and will be exploited by governments, institutions and private parties to create pressure for private companies to take responsibility for dealing with content that is allegedly illegal.

If intermediaries feel coerced, due to such legal uncertainty, to delete Internet content that they fear may be illegal, this is likely to undermine fundamental rights and freedoms, such as freedom of expression, freedom of information, freedom of thought, freedom of creation, the right to education, as well as the rights to privacy and the protection of personal data. Bearing in mind the chilling effect a lack of safe harbours is likely to have on these fundamental rights, we are very concerned at the commercial focus of the questions and the stakeholders expected to answer each question.

We see this in particular in the context of "notice and take-down" systems, where "terms and conditions" of intermediaries are used to reduce the rights of citizens in order to increase the right of the intermediaries to delete possibly problematic web content. In order to respect the current obligations of the EU with regard to the Charter and the upcoming obligations under the European Convention on Human Rights, the Commission must follow these basic principles:

- where an intermediary is not hosting the content (acting as a mere conduit, an access provider or a search engine), it should have no liability for this content, nor should it have any obligations with regards to the removal or filtering of this content as an access provider, it should have neither liability nor obligations with respect to content;
- where an intermediary acts as a hosting provider, its liability with respect to the content hosted should be restricted to its lack of compliance with a court order to take down this content.
- Intermediaries should have no obligation to monitor content.

In summary, content should be dealt with only at its hosting source, and any removal of content at source should only be ordered by a court, following due process of law. Therefore, the provisions of Articles 12, 13, 14 and 15 of the E-commerce Directive should be understood and implemented accordingly.

Specific and or new issues – Search engines:

In terms of content regulation, search engines should be considered in the same way as mere

conduct and access providers, in that they do not host the content the give access to. Obviously, a search engine does "select" the information to a certain extent, according to the user search request. Therefore, the protection should be subject to a requirement on search engine providers to foster transparency about the way in which they provide access to information, in particular by providing the public with information on the criteria used to select search results, to rank and prioritise them. Such a requirement is by no means a call for disclosure of business methods, but simply responds to a need for transparency towards the public.

The Copiepresse v Google case in Belgium (ECDR 5, Brussels Court of First Instance (TGI), 13 February 2007) raises interesting questions about basic levels of diligence that could be expected from complainants. Copiepresse took the case due to publicly available articles in Belgian newspapers being indexed (including a small amount of text from the article) in Google News. Rather than including an instruction in the code of the articles in question that would have prevented them from being indexed (a perfect example of what the legislator meant in Article 13 of the Directive on rules “regarding the updating of the information, specified in a manner widely recognised and used by industry”) the complainant took the case to court and won, on the basis that the text displayed was not subject to a copyright exception under Directive 2001/29/EC.

URL linking:

URL linking is an integral part of the very hypermedia nature of the Internet, therefore the process of linking per se should never be considered as illegal behaviour, unless in specific circumstances to be assessed by court, following due process of law (e.g. in case commercial revenues, “parasitism” or hijacking). The liability for linking to content having been found illegal should be assessed by the court in the same way, on a case by case basis, in order to determine intent.

Web 2.0 services:

Web 2.0 services, which are in constant development, should be addressed using the same general criteria as those currently used in the Directive, so as to keep the general intermediary liability framework easy to understand and to apply. Some of them allow hosting of content while others only access to content hosted elsewhere. Therefore they should lead to the same liability and obligations – or absence thereof – as provided for in relation to other technical intermediary activities.

In June 2007, MySpace in France was successfully sued for infringements of both author’s rights and personality rights. The ruling from the court said that MySpace was a publisher in this

case because it provided a template for the sites it hosts and also embeds advertising in the pages. As a result, MySpace did not benefit from the hosting immunity as implemented in Article 6.I.2 of the French Law on Confidence in the Digital Economy.

In a broadly similar case, also from 2007 (13 July 2007, Tribunal de Grande Instance of Paris), Dailymotion was able to assert its status as a hosting provider but the court made the exceptionally subjective ruling that infringements lead to increased audiences that lead to increased advertising revenues which could have enabled them to install filtering tools which should have prevented the infringements.

Targeted advertising:

When targeted advertising is used by a search engine or a host provider, as an economic model to sustain its activity, the provision of this advertising cannot reasonably be considered to generate "awareness" (in the sense of Article 14 provisions) on the part of the hosting or search provider. Any other approach would be to create an incentive for random, arbitrary, non-transparent and unpredictable filtering obligations on private companies. Targeted advertising should be subject to the same transparency requirement as in the case of search methods.

Administrative authorities:

The repeated references to quasi-judicial decisions being made by unspecified "administrative authorities" in the Directive lead to considerable confusion and lack of clarity at a national level, where the “administrative authority” concept varies significantly within each country. The European Commission should make a detailed analysis of what is expected from Member States in this regard and should ensure that any recommendation be subject to a rigorous assessment following the methodology detailed in the Commission Communication on a Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union (COM (2010) 573). It is inappropriate and contrary to the basic principles of the rule of law that a non-judicial authority can make a definitive ruling on the legality of any given activity.

30. Do you consider that the offer of viewing sporting and cultural events on the Internet, for example by direct streaming, is sufficiently developed? If not, in your view, what are the obstacles to such development?

The offer for sporting and cultural events on the Internet is not sufficiently developed. Worse still, its highly underdeveloped and fragmented state risks promoting unauthorised access to copyrighted material in general.

Citizens have a well-formed sense of fairness and dislike for discrimination. Seeing somebody being given privileges that are not available to all prompts a negative reaction and undermines the legitimacy of whatever law permits or protects this behaviour. In such circumstances, no amount of "education" campaigns in support of respect for intellectual property law - arguing that access to this material that is free for other people is "stealing" - will undo the impression that the legislation is essentially unjust and illegitimate.

As such restrictions are generally national, this problem is arguably even worse in the sporting environment. One major reason that many people would turn to the Internet in order to view sporting events is because they are away from their native country and cannot watch the sporting event on television. As a result, the groups with the most interest in watching a particular sporting event (nationals abroad) see that the content is being provided for free to their compatriots, they see that investment has been made to make the material available online and yet they are prohibited from watching it. In practice, various p2p TV solutions are available which allow circumvention of this national "protection" so the “protection” of the content has limited value, serving only to de-legitimise the legal framework. A second consequence is between citizens based on their level of computer skills – between those who are can use the circumvention tools and the ever smaller number who cannot.

The obstacles appear to be (and this will obviously vary between the cultural and sporting environments) a mixture of the chaotic and fragmented exceptions and limitations regime inflicted on the EU by Directive 2001/29/EC, the chaotic and fragmented rights clearance and collecting society patchwork across Europe and, in the sporting environment, the inability of broadcasters to develop a business model that would draw in the same amount of revenue from online distribution as they earn from satellite broadcasters who sell access to their signals to establishments such as hotels and bars.

The limited scope of the offer of online services, including TV and digital content in general is a major issue in this context and goes far beyond sporting and cultural events. It is regrettable that this issue was not addressed in more detail in this consultation. For a more detailed analysis, we draw your attention to EDRi’s contribution to the Content Online consultation.
http://www.edri.org/files/edri_content_online_consultation100104.pdf

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 E-Commerce Directive does not have any provisions on liability of intermediary service providers. The E-Commerce Directive establishes conditions under which intermediaries will not be held liable (so called “safe harbours”).

While we understand that the purpose in introducing the current provisions was to ensure the necessary legal certainty in order for the European online environment to grow and innovate, the current provisions have proven over time that they lack clarity and precision. Therefore, they have led on the one hand to a number of court cases filed against Internet intermediaries and on the other hand to a chilling effect.

- In some cases, Internet intermediaries (or their associations) have been taken to court following their refusal to take down content following the request by a third private party.
- In other cases, they have been taken to court by authors of content they removed following the request by a third private party.

It should be noted that the latter cases, filed in view of redress, have occurred more infrequently than the former ones. This situation means that countless situations of private censorship are resulting from the current lack of clarity and precision of the Directive's provisions, leading to a chilling effect and resulting in breaches of fundamental rights and democracy.

In all cases, the more effective the methods used by the intermediary, the more invasive they are for citizens, creating a legal quandary for intermediaries as they struggle between being in possible breach of the injunction or in breach of data protection or consumer rights legislation.

Moreover, this situation is hampering the development of a rich European online environment and results in less protection provided to European Internet intermediaries than to, for example, their U.S. equivalents. Furthermore, it leads to less competition in this sector in Europe, since only big Internet intermediary companies can face the current legal risk by investing in large legal departments. As a matter of fact, SMEs and a fortiori non commercial Internet intermediaries cannot face such a burden, and a number of them had to stop their activities.

The lack of clarity surrounding the concept that injunctions must be possible for the purpose of preventing infringements risks creating new barriers to the single market rather than eliminating them.

It is therefore crucial to stop the legal uncertainty resulting by the current provisions of the Directive.

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?

In a coherent legal system, the term "actual knowledge" should not cause any difficulties, as it clearly must refer to a legally sound decision taken by a court that provides the Internet intermediary with the "knowledge" (as opposed to the assumption, suspicion or supposition) that material is illegal. On the other hand, where a measure is used that is lower than a valid notice (an accusation, for example), this will obviously cause problems. The European Commission could usefully clarify this point in guidance to Member States.

The European Commission itself is actually creating some confusion in the DG HOME discussions on (allegedly) illegal online content. It suggests that hosting providers act against websites in the absence of legally sufficient "actual knowledge" in some cases. This approach is also being proposed in the context of the INHOPE network. While this is problematic enough in the policy areas for which this is suggested (racism/xenophobia, child abuse and terrorism), it would be incoherent to take a different approach for accusations in other contexts but very disproportionate to take the same approach.

Even in the context of a correct interpretation of the term "actual knowledge", there is no reason for intermediaries to get involved in activities which are in no way related to their business purpose, such as spontaneous searches for material or behaviour that might be illegal. If undertaken by intermediaries, such activities not only would breach their trusted contractual relationships with their customers, but also would breach European privacy and data protection laws: while the collection and processing of their customers personal data is necessary and lawful when used for the provision of the contracted service, they would breach the principles of proportionality and purpose limitation if used in the course of monitoring online activities, and would lead to arbitrary sanctions against clients.

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?

We are not aware of any problems with regard to Article 13(1)(e) of the Directive, nor of any actual application of this provision. In any case, this provision does not seem to be realistically applicable, given the effective operation of the caching activity. It could be replaced by a provision requiring frequent periodic refreshment of the caches, so that any content removal at source would be automatically taken into account. It should be noted in any case that such refreshing of caches are necessary for reasons related to the provision of updated content on the one hand and to the management of servers on the other.

With regard to article 14(1)(b), the YouTube/Vividown case showed a lack of consistency between the general safe harbour intended to be offered by the Directive and the protection of

intermediaries in cases that are covered by exceptions in the Directive, such as the general data protection Directive.

The core problems with Article 14(1)(b) of the Directive appear to be:

a. A lack of common understanding that "knowledge" can only realistically be based on a judicial decision and
b. A lack of research regarding the extent to which, in relation to content depicting serious crimes, expeditious take-down of illegal content may serve to discourage or replace effective action by organs of the state. This danger is shown clearly by the DG Home draft recommendations on notice and take-down of criminal content, which suggested (in relation to content reported by citizens that is unquestionably illegal in the eyes of the hosting provider) that the provider "should" contact law enforcement authorities or a hotline. In this so-called "public-private partnership" the intermediaries would undertake to act as judge, jury and executioner while it was not proposed that the public authorities would undertake to perform any action whatsoever.

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?

As an example, France has implemented a notice and take-down procedure in its national law transposing the E-Commerce Directive (Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, NOR: ECOX0200175L, JORF). The related provision is Article 6.I.-5 of the law. Abusive notifications are punished by law (Article 6.I.-4). See also the French Constitutional Council ruling on this law at:
http://www.conseilconstitutionnel.fr/decision/2004/2004496/index.htm.

Furthermore, this notice and take down procedure has no other objective than to organise private censorship by third parties, as EDRi member IRIS commented at different steps of the draft law discussion (see dossier at: http://www.iris.sgdg.org/actions/len and more specifically:
http://www.iris.sgdg.org/actions/len/point-len0203.html#3.2 and
http://www.iris.sgdg.org/actions/len/point-len0304.html#5).

While this procedure, as implemented in the French law, might provide better – though certainly not full – legal certainty to Internet intermediaries, it actually encourages content removal without any proof of the illegality of content, precisely because the intermediaries indeed feel more protected when receiving such a notice provided by law. The final result is not only to encourage breaches of freedom of expression and other fundamental rights, but also to switch the burden of proof from the third party to the author of the content, who has to respond and

show that his/her content is indeed legal. This change in the burden of the proof also occurs in countries having implemented systems of counter-notice and put-back.

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?

Since there is no transparency requirement from host providers, either for the accounting – or even statistics - of received notifications, or on the follow-up actions they might have taken, it is impossible to answer this question.

57. Do practices other than notice and take down appear to be more effective? ("notice and stay down"13, "notice and notice"14, etc)

It appears self-evident that illegal content is most effectively dealt with by swift and efficient investigation, prosecution and removal using publicly accountable judicial process and the rule of law.

"Notice and takedown", by contrast, can only be a very poor and dangerous "second best" and carries with it the very serious risk of subtractionality which, to the best of our knowledge, has never been studied and balanced against the potential gains of this approach.

Detailed research is urgently needed on the damage to fundamental rights, such as the rights related to communication, caused by the existing "notice and take-down" regimes. The research carried out by EDRi member Bits of Freedom in 2004 (http://www.bof.nl/docs/researchpaperSANE.pdf) and "How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation", 2002 http://www.rootsecure.net/content/downloads/pdf/liberty_disappeared_from_cyberspace.pdf) indicate that a failure by the Commission to clarify and improve the "notice and takedown" approach currently in force may well represent a failure of the Commission's obligations on respect for the Charter on Fundamental Rights, as detailed in the Communication on the Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union COM (2010) 573.

Practices such as “notice and stay down” or “notice and notice” do not appear to better protect fundamental rights than the “notice and take down” scheme. “Notice and stay down” implies in addition a monitoring obligation from Internet intermediaries, so as to ensure that the content does not appear elsewhere or reappear online. “Notice and notice”, while seemingly more sympathetic to freedom of expression, since it does not involve any content removal by the Internet intermediary, actually leads to a chilling effect, to an even greater extent than “notice

and take down". Furthermore, it is incompatible with the current provisions of the Directive (liability upon "actual knowledge", when "actual knowledge" may derive from "notice" by any other party than a court), and would be redundant and useless in the scheme advocated by EDRi, i.e. content removal following a court order.

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

As an example, France has implemented such provisions in its national law transposing the E-Commerce Directive (Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, NOR: ECOX0200175L, JORF). The relevant provisions are Article 6.I.-7 and Article 6.I.-8 of the law. After a general monitoring obligation was proposed during the discussion of the draft law, the final provisions are limited to the extent allowed by Article 15 of the Directive. It results that the French law provides for targeted surveillance upon request by the judicial authority.

It should be noted that in the French legal system, "judicial authority" ('autorité judiciaire', in French) does not necessarily mean a judge, nor a court ruling following due process. The "judicial authority" in France can also be understood as the public prosecutor (not independent but under the authority of the ministry of Justice, i.e. the executive power) in the course of a preliminary investigation or a legal decision by a judge upon request from a third party ('ordonnance sur requête').

Furthermore, the French law requires, in the above mentioned provisions, access and host providers to help fighting some crimes by providing a hotline where Internet users can report such alleged crimes to them. Access and host providers should report such information to public authorities.

The crimes that are covered relate to: crimes against humanity, incitement to racial hatred, child abuse material, incitement to violence, notably against women, and offences against human dignity. In addition, access and host providers should "contribute" to the fight against a list of press infringements (referred to in the French law provision).

This example shows that current Article 15 of the Directive lacks the needed precision to pre-empt easy circumvention by some Member States. Indeed, article 15 does not prevent Member States from imposing a monitoring obligation on service providers "in a specific case" or "to apply duties of care [...] in order to detect and prevent certain types of illegal activities". It is unclear what is meant by a "specific case" and by "certain types of illegal activities". How "specific" does a monitoring duty need to be?

As another example, the lower court in the Belgian Scarlet/Sabam case imposed an obligation to monitor which was specific insofar as it sought to filter out all but "approved" files while it was general insofar as all files needed to be checked before being permitted or rejected. If such an approach is permissible under the Directive, then the scope of the "in no way involved" limitation must be understood in the widest possible sense in order for the safe harbour provisions to retain any meaning.

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?

It is far from clear what "effective" might mean in this case.

In the first instance, it is clear that the implementation of any widespread filtering technology will bring data protection implications, as detailed by the EDPS in the recent hearing on child exploitation in the European Parliament and in its opinion on the child exploitation Directive. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-05-10_Child_Abuse_EN.pdf. There are serious doubts as to the fundamental rights legitimacy of existing filtering systems.

Furthermore, restrictions on communication must be subject to law, in order to be in compliance with Article 10 of the European Convention on Human Rights. Indeed, the analysis undertaken by the OSCE raised several serious doubts about the legality of filtering under the European Convention on Human Rights (http://www.osce.org/documents/rfm/2010/01/42294_en.pdf).

Italy has a legal framework for filtering beyond the injunctions provided for in the E-Commerce Directive. France has also implemented some provisions for filtering in its national law transposing the E-Commerce Directive (Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, NOR: ECOX0200175L, JORF). The related provisions are Article 6.I.-8 of the law. They allow for the “judicial authority” (see comments on this authority in EDRi answer to question 58 above) to require access provider (when the host provider is in a foreign country)” to undertake any measures to prevent or stop a damage caused by a given online content”. This clearly means a requirement to filter (block) online content. As a matter of fact, this provision was adopted as an answer to the demands of rights-holders, two years before the adoption of the DADVSI law and five years before the HADOPI law.

Thirdly, the measurement of "effectiveness" is a very complex one with regard to filtering. For example, both the UK secret service (http://www.timesonline.co.uk/tol/news/uk/crime/article6885923.ece) and the United States

secret service (http://www.techdirt.com/articles/20101006/04135311311/us-intelligence-agencies-angry-at-france-over-three-strikes-worried-it-will-drive-encryption-usage.shtml) complained about allegedly serious damage to effective law enforcement that would be caused by surveillance measures undertaken under the UK Digital Economy Act and French HADOPI Act respectively. Filtering would be likely to cause the same negative impact.

Filtering has a cost in relation to "mission creep" as it will spread to cover ever more irrelevant and disproportionate uses, it has the cost for law enforcement detailed by the UK and US secret service, it has a cost for Europe's credibility in the international fight for democratic and open networks and it has a cost in terms of probable breaches of the Charter on Fundamental Rights and the European Convention on Human Rights.

Could the surveillance be considered "effective" if it was causing that level of unintended consequences? Could the surveillance be considered "effective" if it only served to push Internet users to (probably automatic) encryption?

In the history of Voice over IP, several developing countries "effectively" filtered out VoIP traffic, in order to protect monopoly call termination traffic. As a result, Skype, which is effectively unblockable (due to encryption and other techniques) was developed. It could hardly be argued that this filtering was "effective" in anything other than the short term and ultimately rendered policing much more difficult. It also gave Skype a "first mover advantage" in the marketplace, inflicting long-term economic damage on the very operators that the filtering was meant to protect, who relied on filtering rather than developing their own alternative and innovative products.

For all these reasons, the Council of Europe adopted on 26 March 2008 its “Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters” (https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2008)6). This document, which provides recommendations to member States to inter alia, “refrain from filtering Internet content in electronic communications networks operated by public actors for reasons other than those laid down in Article 10, paragraph 2, of the European Convention on Human Rights, as interpreted by the European Court of Human Rights” and “guarantee that nationwide general blocking or filtering measures are only introduced by the state if the conditions of Article 10, paragraph 2, of the European Convention on Human Rights are fulfilled”. The Recommendation is complemented by an explanatory report which assesses the many flaws of different filtering techniques (https://wcd.coe.int/ViewDoc.jsp?Ref=CM(2008)37).

Other provisions of the Recommendation are intended as guidelines to Internet intermediaries.

Furthermore, the European Internet Services Providers Association (EuroISPA) has cooperated with the Council of Europe to defines “Human rights guidelines for Internet service providers” (http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2008)009_en.pdf).

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?

No, it would not make a useful contribution and yes, it could make things worse. See the answer to question 59 for some explanation.

61. Are you aware of cooperation systems between interested parties for the resolution of disputes
on liability?

A mediation services exist in France (http://www.foruminternet.org/particuliers/mediation), but is does not address intermediary liability issues. However, it may deal with disputes among individuals in cases related to privacy. In 2009, these cases accounted for 0.8% of all mediation cases dealt with by the service. The majority of cases (94%) concerned consumer issues in the course of e-commerce activities (contractual disputes).

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

Some countries have extended the liability regime for hyperlinks or search engines, without a proper explanation why that was needed. See for example article 15 of the Romanian E-commerce Law 365/2002. To our knowledge this article was actually never enforced in practice.

Art.15: Information searching tools and other links with other web sites
(1) The information society service provider facilitating the access to the information supplied by other service providers or by the recipients of the services offered by other suppliers, by making available for the recipients of his service some information searching tools or links to other web sites, is not liable for the respective information, in any of the following conditions is fulfilled:
a) the provider is not aware of the fact that the activity or information to which is grants access is illegal and, as concerning the torts, he is not aware of any facts or circumstances showing that the respective activity or information could prejudice the rights of a third party;
b) being aware of the fact that the respective activity or information is illegal or of facts showing that the respective activity or information might prejudice the rights of a third party, the provider

acts rapidly to eliminate the access possibilities offered or to block its use.
(2) The service provider is responsible for the respective information when the illegal character of it has been found by a decision of a public authority.
(3) The provisions of item (1) do not apply in the situation when the recipient acts under the order or command of the service provider.

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

See answer to question 62 above.

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

The cloud computing hosting makes the data available in several jurisdictions, in general only known by the service intermediary, which makes notice and take-down actions impossible, without a proper court decision and proper international agreements on the competence of jurisdictions.

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?

As clearly stated in many parts of its answer to this consultation, EDRi does not think Articles 12 to 15 clarify enough the position and obligations of intermediaries. In particular, this hampers the development of e-commerce services by SMEs and by non commercial organisations (the latter case may apply in case of, e.g. NGOs selling their publications). The legal uncertainty these provisions create is also of concern to some bigger online service providers and Web 2.0 platforms providers.

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 case15. 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?

Yes. However, based on experience from some Member States, such as France (cases related to the “Google suggest” feature of the search engine, see below), it may be valuable for the

Commission to clarify that automated processes do not give knowledge of, nor control over, content to the provider. The explanation provided in Recitals 42 and 43 of the Directive is informative in this regard.

It would also be valuable to clarify that the use of (and profit from) targeted advertising cannot logically be considered to have given the hosting provider any "knowledge" or "awareness" of illegal content, within the understanding of these terms in the Directive. Any suggestion that targeted advertising does create "actual knowledge" can only lead to automated blocking of content based on keywords, which would be both disproportionate and ineffective.

Here again, as already stated, this clarification should include a requirement on search engines providers to foster transparency about the way in which they provide access to information, in particular by providing the public information on the criteria used to select search results, to rank and prioritise them. Such a requirement is by no means a call for disclosure of business methods, but simply a need for transparency towards the public.

French cases related to the “Google suggest” feature are listed below (in all cases Google was found liable):

- Direct Energie vs. Google Inc., Tribunal de commerce de Paris (référé), 7 May 2009 (so-called “Direct Energie scam”, http://legalis.net/spip.php?page=jurisprudence-decision&id_article=2687
- Google Inc. vs. Direct Energie, Cour d'Appel de Paris, 9 December 2009 (Appeal in so-called “Direct Energie scam”, http://legalis.net/spip.php?page=breves-article&id_article=2804)
- CNFDI vs. Eric S., Google Inc., TGI Paris (référé), 10 July 2009 (so-called “CNFDI scam”, http://legalis.net/spip.php?page=jurisprudence-decision&id_article=2694)
- CNFDI vs. Eric S., Google Inc., TGI Paris (fond), 4 December 2009 (so-called “CNFDI scam”, http://legalis.net/spip.php?page=breves-article&id_article=2817)
- X vs. Eric S., Google France, Google Inc., TGI Paris, 8 September 2010 (defamation of an individual, http://legalis.net/spip.php?page=jurisprudence-decision&id_article=2985)

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?

There is a logical problem in permitting administrative or legal authorities to impose "general" obligations to monitor when the legislator has decided that such an approach is inappropriate.

The imposition of a general obligation to monitor via court decision, as proposed in the Scarlet/Sabam case brings with it the requirement for intermediaries to have scalable and efficient tools to undertake this monitoring.

The possession of such tools will then, logically, make it easier for intermediaries to "voluntarily" use these tools for the purposes of filtering out, for example, content provided by competitors or imposing on themselves a monitoring obligation in order to avoid court costs and/or to ensure that they will not be held liable for content that may subsequently be considered to be illegal.

Ultimately, therefore, any obligation to monitor imposed by administrative or legal authorities will lead to generalised monitoring which is in obvious and diametric opposition to the clear intention of the legislator.

Injunctions should be subject to clear limitations, in order to ensure coherence, clarity and predictability. In particular:

- such relief should fulfil the requirements of proportionality and subsidiarity from the perspective of fundamental rights;
- it should be appropriate and strictly necessary to prevent further damage caused by specific instances of unlawful information.
- should not be imposed if it would render the applicable safe harbour meaningless in practice. A requirement on ISPs to police the content over their network is an example of this. It does not make sense to have a safe harbour for mere conduit services if those services can nonetheless be required to police their networks.

EDRi considers that the Council of Europe Recommendation CM/Rec(2008)6 on Internet filters constitute a good basis to define these limitations.

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?

Yes. However, this classification should be extended to intermediary services and intermediation activities not currently dealt with by the Directive, such as search engines, linking, Web 2.0 services... as stated in EDRi comments in the introduction of its answer to this consultation.

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.

No.

The first problem is that counterfeiting and unauthorised access to digital content (a.k.a. "piracy") are two entirely different phenomena. The economic and health implications of the consumption of a counterfeit medicine and an unauthorised copy of a piece of music are radically different. Failure by policy-makers to recognise the basic differences between two very dissimilar phenomena will result in one or other infringement being dealt with either disproportionate (and counterproductive) severity or disproportionate laxity.

Unauthorised access to content has grown due to inflexibility of content providers both in the provision of content (there were as few as 50 licensed music outlets in 2003 - source: IFPI digital music report 2010), the format of music (especially through the use of digital locking systems and/or spyware on legally purchased music) and the cost of digital music (which fails to take account of the savings made from this delivery method). This problem has been exacerbated by oppressive measures such as HADOPI in France or its "voluntary" vigilante version in Ireland. In this context, any lack of investment in law enforcement prevents a bad situation from being made even worse.

However, lack of investment in law enforcement with regards to combating crimes as serious as child abuses, in the course of due legal process, is the source of “devolved” or “delegated” regulation to private parties (generally wrongly though purposefully referred to as “self-regulation” or “co-regulation”), that is highly contestable in EDRi’s opinion for all the reasons detailed throughout this document.