November 5th, 2010

# Legal Liability of Internet Service Providers and the Protection of Freedom of Expression Online

**Response to the European Commission's consultation on the e-Commerce directive.**

## About La Quadrature du Net

La Quadrature du Net is a France-based **advocacy group that promotes the rights and freedoms of citizens on the Internet**. More specifically, it advocates for the adaptation of French and European legislations to respect the founding principles of the Internet, most notably the free circulation of knowledge. As such, La Quadrature du Net engages in public-policy debates concerning, for instance, freedom of speech, copyright, regulation of telecommunications and online privacy.

In addition to its advocacy work, the group also aims to foster a better understanding of legislative processes among citizens. Through specific and pertinent information and tools, La Quadrature du Net hopes to encourage citizens' participation in the public debate on rights and freedoms in the digital age.

You can contact us at: contact@laquadrature.net

## Executive summary

The 2000 e-Commerce directive, which sets a legal framework for most online activities, created a legal security for telecommunication services and even more importantly for host providers through ad hoc liability exemptions (article 12 to 15). By doing so, the directive created a special legal framework distinct from the one regulating traditional media and interpersonal means of communications, and enabled strong innovation and growth in the online sector.

In the past years, however, legislative, administrative as well as judicial decisions have led to diverging interpretations regarding the scope of the liability exemptions granted by the directive. In our opinion, the main reason for these diverging interpretations does not lie in the ambiguity of the provisions in the original directive (though some may need to be adapted to take in account new technologies and uses). Rather, this trend results from a concerted offensive of interests that do not accept the philosophy of the directive. It must be stopped if freedom of expression online is to be protected, and innovation as well as economic growth encouraged.

We substantiate this claim in our answers to the European Commission's consultation.

- We stress that overcoming the present growing legal uncertainty while preserving the fundamental freedoms will call for a firm reassertion and a new and more detailed formulation for the core principles of the directive. The directive should expand the liability exemptions to new categories of online service providers and create a framework that can accommodate new and still unknown services.

- In particular, while the provisions regarding the termination of an infringement can probably be clarified without substantial change, the possibility of injunctions for preventing an infringement must be reviewed to make sure that they do not result in a *de facto* presumption of infringement, in particular in the area of copyright or if they involve filtering systems. Such injunctions will have to be effective, proportionate and correspond to the least restrictive alternative. In general, we take the view that for all online speech, there must be a systematic presumption of freedom of publication.

- Expeditious procedure can be put in place to prevent the continuation of an infringement in the very rare cases where it is associated with irreparable damages, such as in the case of child pornography. However, even if these cases of very serious criminal offenses, these procedures cannot unilaterally rest on obligations or actions imposed on private parties. To abide by the rule of law, such take-down procedures must at least involve an order from an administrative authority, whose preemptive action must be rapidly followed by confirmation of illegality by an independent and impartial tribunal.

- In all other cases, notifications to service providers regarding the existence of possibly infringing content should not lead, as is often the case, to a systematic action of removal by the service provider (the host provider should first try to contact the person responsible for the posting of the allegedly illegal information). We suggest different principles to codify take-down procedures and stress that adequate and dissuasive sanctions should be provided in EU law against abusive notifications.

In spite of the growing trends to turn Internet service providers in police auxiliaries – whether it is at the national, European or international level (with initiatives such as the Anti-Counterfeiting Trade Agreement) – we urge the Commission to take the opportunity of this long-awaited reform of the e-Commerce directive to protect the fundamental freedoms of citizens, thereby sustaining a legal environment conducive to innovation and growth in the online ecosystem.

# Questions

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

Overall, given the widely differing transposition of the directive, it seems that indeed member States' lawmakers and courts have had difficulties with the interpretation of the directive. In turn, the disparity has led to a fragmented regulatory framework across the EU, with some member States offering sound protections for online freedom of expression while others opted for much less

protective provisions. In particular, “injunctions aimed at preventing an infringement”, the notion of “actual knowledge” or the requirements attached to “notice and take-down” demands have raised difficulties which are discussed in the following questions.

**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 the directive it is unclear whether “actual knowledge” refers to knowledge of the allegedly infringing material or actual knowledge of the illegality of the material. As a consequence, the notion of “actual knowledge” has been subject to different interpretations of the level of awareness of service providers necessary to trigger the obligation to “expeditiously” remove the problematic information. In particular, national lawmakers and judges have faced the difficulty of determining how a host provider could obtain actual knowledge of the illegality of a given content without being presented with a court order.

Several national courts have created the category of “manifestly” of “obviously” illegal information that should be removed as soon as the existence of such content is notified to the service provider, even when there is no court order declaring the said-content to be illegal. For instance, the French Constitutional Council, justified the creation of such a category by stressing the difficulty, “even for a lawyer” to characterize a given information as illegal.

> *“In most cases, because of the frequent difficulty of assessing the legality of content, the host provider does not have – even when factual knowledge of that content would be obtained – neither the human, technical or financial, or in the absence of intervention by legal authorities or administrative authorities, the capacity of legal analysis sufficient to meet the obligations [of removing the allegedly illegal content].*
>
> *The characterization of a malicious message can be difficult, even for a lawyer. Under these conditions, host providers might be tempted to escape their obligations by ceasing to make available content subject to claims by a third-party, without examining the merits of such claims. By doing so, they would violate the freedom of communication.”*[1]

Failure to remove such manifestly illegal information triggers the liability of the host provider. Most national judges have created similar categories to types of content for which the provider can determine the illegality and expeditiously remove the said content in the absence of a court order. Most often, the types of content that are included in this category are, or at least were, limited to child abuse and hate speech. The restrictive nature of this category has helped ensure

1 *“En raison (…) de la difficulté fréquente d'apprécier la licéité d'un contenu, l'hébergeur ne disposerait dans beaucoup de cas, même lorsque la connaissance factuelle de ce contenu lui serait acquise, ni des moyens humains, techniques ou financiers, ni, en l'absence d'intervention des autorités juridictionnelles ou administratives compétentes, de la capacité d'analyse juridique suffisants pour honorer les obligations [de suppression des contenus litigieux]. La caractérisation d'un message illicite peut se révéler délicate, même pour un juriste. Dans ces conditions, les hébergeurs seraient tentés de s'exonérer de leurs obligations en cessant de diffuser les contenus faisant l'objet de réclamations de tiers, sans examiner le bien fondé de ces dernières. Ce faisant, ils porteraient atteinte à la liberté de communication”.* Les Cahiers du Conseil constitutionnel , comentaries on the decision n° 2004-496 DC of June 10th, 2004 , Cahier n° 17 , p. 4. Address : http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2004/2004-496-dc/commentaire-aux-cahiers.12885.html

that the extra-judiciary regulation of online content would remain marginal.

However, this protective regime is undermined by its extension of the types of content that can be deemed "manifestly illegal". For instance, in France, judges have gone beyond the above-mentioned types of content and condemned host providers for not expeditiously removing copyright-infringing[2] and defamatory content[3]. There is more: in a 2008 ruling[4], a Parisian court went against the Constitutional Council decision by expanding the obligation a host provider to "act expeditiously" to remove content that is "likely" to be unlawful.

Consequently, it appears that the types of content that can be directly taken down upon notification is rapidly broadening, which in turns tend to increase the extra-judiciary repression of abuses of freedom of expression by expanding the role of host providers. This is dangerous when one consider that in a country abiding by the rule of law, only a judge should be entitled to declare a given use or publication of a piece of information to be illegal. The creation of the "manifestly illegal" category already represents a departure from this principle, and such exceptions should be narrowly limited.

**Recommendation 1:** The reform of the e-Commerce directive should be an opportunity to reassert the role of the judiciary to pronounce measures interfering with the freedom of expression on the Internet. EU lawmakers must also put an end to the ongoing jurisprudential "mission creep" expanding the role of host providers to regulate online content.

In the case of very serious criminal infractions, the administrative authority should be the only party competent to order the removal (take-down measures) of "manifestly illegal" content to prevent the continuation of the alleged infringement. At this point, the content will only be allegedly illegal. The publisher of the content will have to be prosecuted before the judiciary in order to assert their illegality of the said-content and, if it is indeed illegal, take appropriate measures to repress the abuse of freedom of expression.

Such competence of the administrative authority to order the preventive take-down of "manifestly illegal" content should be an exception to the general principle that only only a independent and impartial judiciary court is competent to restrict freedom of expression online. As such, the "manifestly illegal" category should be limited to very serious criminal offenses, such as child pornography.

Also, it should be asserted that if a host provider acquires knowledge of the illegal nature of a given content and decide to act to prevent it), this should not be considered as a proof that it was monitoring and checking content, which would deprive him from the liability exemption.

2 Cour d'appel de Paris, June 7th, 2006, *Tiscali Media v.Dargaud.*

3 Tribunal de Grande Instance de Paris, November 15th, 2004, Juris Data n° 2004-258504

4 Tribunal de Grande Instance de Paris, 15 avril 2008, *Jean-Yves Lafesse c/ Dailymotion.* http://www.juriscom.net/jpt/visu.php?ID=1057

" *Contrairement au tribunal qui ne peut se fonder sur une vraisemblance de titularité des droits pour apprécier des actes de contrefaçon et prononcer une éventuelle condanmation, les hébergeurs doivent devant la vraisemblance des actes de contrefaçon et la vraisemblance de titularité des droits résultant éventuellement des mentions portées sur les supports de diffusion des oeuvres communiqués, apprécier le caractère illicite des contenus mis en ligne. La transmission des documents exigés par l'article 6-I.5 de la LCEN par les auteurs ou les producteurs s'estimant contrefaits a pour effet de créer une nouvelle obligation de vérification des contenus argués de contrefaçon au regard des droits allégués, nouvelle obligation qui pèse sur les hébergeurs qui ne peuvent se contenter d'attendre une éventuelle décision de justice et qui doivent dès lors agir promptement pour faire cesser cette atteinte sur la seule base du caractère vraisemblable de la contrefaçon*".

**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?**

As far as we know, the interpretation of the term “expeditious” has not created important difficulties. Rather, the issue has to do with the situation that triggers the obligation to expeditiously remove the content. As mentioned before, “expeditious action” used to be required only when the content was “manifestly illegal”, but this state of play is rapidly changing, which in turn creates great legal uncertainty for host providers.

**Recommendation 2:** As mentioned above, we take the view that such expeditious action to remove online content should only be mandatory when the lawfulness of the given content is asserted, i.e. after a court order has declared it to be illegal, or when the content is manifestly illegal upon notification by an administrative authority and prior to a subsequent ruling confirming the unlawfulness of the publication of the content.

As long as the content is only “allegedly” illegal, there should be no obligation for the host provider to act expeditiously to remove the content (see our view on notice and take-down procedures in our answer to question 56), since the illegal nature of the content has not been established.

**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?**

Most Member States have adopted formal requirements regarding notice and take-down procedures, either through law or case law. Such requirements are extremely useful to help ascertain the credibility of the notification sent to the intermediary. However, some member States rely to a great extent on self-regulation, which is partly encouraged by the directive (article 16). Self-regulation leads to discrepancies regarding the form of the notification, and therefore to legal uncertainty for host providers, which adversely affect the freedom of expression online.

**Recommendation 3:** The Commission could usefully review existing requirements and best practices in order to provide a EU-wide framework to define notice and take-down formal requirements (addressee, full name and address of the sender of the notice , accurate identification of the allegedly illegal information, nature of alleged infraction, etc).

**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 lack of specific requirements in EU law regarding the procedures for notice and take-down have led to important discrepancies in the way providers handle requests for the removal of allegedly illegal information (when the content is neither manifestly illegal nor qualified as such by a judge).

Research projects carried on in 2003-2004 showed that the majority of host providers, upon

receiving a demand for take-down, did not check the veracity of the alleged infraction, and that they removed content that they they could have easily determined to be legal[5]. In this context, the e-Commerce directive should be upgraded to define in a more comprehensive way notice and take-down procedures, with the aim to ensure that freedom of expression will be put first. In the absence of legal requirements, the provider will be tempted to deal negligently with the request and minimize all legal risks by taking down the content.

As Alhert, Marsden and Yung explained in 2004:

> *"The quandary for the ISP is whether to strictly investigate all claims of legal infringement, which is higher cost to itself in legal and forensic resources, or to adopt a more self-serving, cheaper and easier regime. To save costs and liabilities, the ISP may remove content immediately upon notice in order to protect itself against liability or to satisfy content consumers. The ISP is encouraged to become a censorship body, to avoid liability when they choose to take down the information from a website upon receipt of a claim."*[6]

**Recommendation 4:** To make sure that providers will protect the free speech of Internet users, the directive should be amended to. In 2004, Sjoera Nas proposed[7] that:

– In the absence of court order, providers should be obliged to give their customers a reasonable time to respond.

– While waiting for the answer, content should not be be removed, except in case of manifestly illegal information, immediate danger or proven financial damages.

– In case of counter-notice on the part of the customer, the provider should notify the third-party who sent the initial take-down request that the customer is challenging their claim, and propose that the case be referred to a court.

– EU law should also provide sanctions for abusive notice and take-down demands as well as for wrongful take-downs on the part of the provider. For small providers who have difficulties meeting the financial cost of in-house legal expertise, they should be encouraged to pool resources by creating cross-industry organizations able to advise them on notice-and-take-down matters.

– Lastly, providers should provide their users with clear information on their notice and take-down procedures.

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

See question 56. A "notice and notice" procedure, whereby the provider must inform the person who uploaded content violating the law so as to give him the opportunity of a counter-notice, is preferable.

5 Nas Sjoera, 2004, "The Multatuli Project : ISP Notice & Take Down", Sane. Address: http://www.bof.nl/docs/researchpaperSANE.pdf

6 Christian Alhert, Chris Marsden, and Chester Yung. "How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation", p. 7 (2004).

7 Nas Sjoera, op. cit.

We note that somewhat similar procedures currently exists in Japan, where the provider has the obligation to notify the alleged infringer. The latter is offered the opportunity to contest the claim of infringement. If the alleged infringer agrees to take the material down, or if no counter-notice is received within seven days, the content is removed.

In Canada, a procedure whereby the first and primary role of the provider was to forward the notice to the user who published the information was also considered in 2005 and 2008. It failed to become law as a result of the federal elections[8].

**58. Are you aware of cases where national authorities or legal bodies have imposed general monitoring or filtering obligations?**
**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 provisions regarding injunctions aimed at preventing an infringement represents another major difficulty in the way the e-Commerce directive has been interpreted. Articles 12 to 14 of the directive do not forbid national courts or administrative authorities to require a given service provider to terminate or prevent an infringement on a case-by-case basis. This possibility to order measures "preventing an infringement" has led to an important number of injunctions leading to broad Internet filtering practices – similar to censorship – which harm the protection of fundamental rights in the EU (see answer to question 60).

**National transpositions.** Firstly, national transpositions provides this possibility. For instance, in France, the law for the confidence in the digital economy[9] provides that courts with the power to order all measures to prevent or halt a damage[10]. Such a transposition of the e-Commerce directive's provisions regarding the prevention of infringements was reasserted in the context of the HADOPI law aimed at tackling the sharing of cultural works over the Internet. In its article 10, the law grants judges the power to order "*all measures needed to prevent or halt such damage to a right of authorship or a related right, against any entity able to help remedy it*".

**Case law.** Secondly, judges are struggling to put into practice this possibility granted by EU law while respecting fundamental freedoms, such as freedom of expression or privacy. The Scarlet/SABAM case in Belgium, the judge ordered that the IAP "*make the infringements of copyright cease by making it impossible, in any form, via peer-to-peer software, for its clients to send or receive electronic files containing musical works from the [collecting society] SABAM repertory*". After this first instance ruling that ordered Belgian IAPs Scarlet to prevent the sharing of copyrighted works over the Internet, the Brussels Court of Appeal has cautiously asked the European Court of Justice to clarify whether *a priori* filtering practices are legal under EU law[11].

8 See DeBeer Jeremy F. and Clemmer Christopher D., 2009, « Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries? », *Jurimetrics*, vol. 49, n° 4, p. 386. Address : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1529722

9 Loi pour la confiance dans l'économie numérique of June 21st, 2004.. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&dateTexte=

10 Article 6-I-8: "*L'autorité judiciaire peut prescrire en référé ou sur requête, à toute personne mentionnée au 2 ou, à défaut, à toute personne mentionnée au 1, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne*".

11 See question from the Brussels Court of Appeal, dated February 5th, 2010, Ref C-70/10. International Law Office, October 4th, 2010, « Courts look to ECJ as fight against illegal downloading continues », *internationallawoffice.com*. Address : http://www.internationallawoffice.com/newsletters/detail.aspx?

This preliminary ruling is of great importance for the protection of fundamental rights online.

In another instance where preventive filtering has been mandated through a court order, a Hamburg court found in September 2010 that video host provider YouTube was liable for the copyright infringing content uploaded by its users, especially because the platform can be used anonymously[12]. The court said that YouTube had to pay damages for not having prevented and blocked the upload by its users. Although YouTube's owner, Google, has appealed the ruling, this precedent risks further eroding the principle of the directive and could lead to a general monitoring obligation, which is expressly prohibited by article 15 of the e-Commerce directive.

In France, in the 2007 the French film company Zadig Productions sued Google Video regarding the repeated posting of some of its copyrighted material[13]. Google had complied with each of the notice-and-take-down requests sent by Zadig. However, Zadig argued before the court that Google should have established a system to prevent the posting of its content, effectively calling for an *a priori* filter on user-generated content. Nevertheless, in spite the fact that the judge recognize Google had acted expeditiously to remove the content, the court said it was liable for not having prevented the repetition of the infringement. The court held that even "*'if the [multiple postings] are attributable to different users, their content (...) is identical*"[14]. Google was required, through a careful wording, to use "*targeted and temporary surveillance*" to "*avoid damage or abate damage caused by [specific content]*". Of course, establishing such a system for one specific content is likely to lead other rights holders to sue Google for similar allegedly infringing content, increasing the pressure on Google to adopt a general monitoring system. As a Méhaud explains:

> *"This decision drastically restricts the scope of the limitation of liability (...) and places a heavy burden on hosting providers to maintain sophisticated systems for ongoing monitoring of content posted by users."*[15]

Also, after a similar ruling against host provider Dailymotion (discussed in our response to question 68), in which Dailymotion was qualified as a publisher by the French judge, Dailymotion adhered to the "Principles for User-Generated Content"[16], negotiated between some major rights holders (including CBS, Disney, Fox Entertainment, NBC Universal, Sony Pictures, and Viacom) and intermediaries (including Microsoft, Crackle, MySpace, Veoh, and Dailymotion). These principles require the websites hosting user-created content to implement filtering and fingerprinting technology to block ostensibly infringing files, to promote public education relating to copyright, and to remove copyrighted material that had been uploaded before the agreement. In exchange for host providers' efforts to protect copyright, the rights holders have agreed not to sue operators that adhere to the policy. Hence, because of the legal pressure resulting from a dangerous case law departing from the liability exemptions provided by the e-Commerce directive, we have come to a situation in which service providers are compelled to deploy preventive filtering systems.

**Calls for administrative injunctions.** Although this emerging case law is worrying, the development of administrative injunctions blocking or restraining access to Internet content is

g=c4173f67-7f9a-4063-8f62-a884b1149157#3

12 Associated Press, September 3rd, 2010, « German court rules against YouTube over copyright », Address : http://news.yahoo.com/s/ap/20100903/ap_on_hi_te/eu_germany_youtube

13 Tribunal de grande instance, Zadig Prod. v. Google, October 19th, 2007.Address: http://www.juriscom.net/documents/tgiparis20071019.pdf.

14 DeBeer Jeremy F. and Clemmer Christopher D., *op. cit.*, p. 400.

15 Mehaud Jeanne, 2007, « Saga Internet Hosting Provider Liability France », *Bird & Bird Continuing*. Address : http://www.twobirds.com/Finnish/News/Articles/Sivut/Continuing_saga_internet_hosting_provider_liability_France.aspx

16 http://www.ugcprinciples.com/

even more dangerous since it excludes the procedural guarantees attached to a fair trial. Such administrative injunctions are exemplified by the LOPPSI bill in France, the Digital Economy Act in The UK, or the questionnaire sent by the Council Presidency to member states in February 2010, which displayed a growing interest in filtering on the part of European lawmakers, including administrative filtering[17].

**Calls for more "auto-regulation".** Lastly, the prohibition to impose a general obligation to monitor Internet user's online activity is indeed undermined by the persistent calls for more "auto-regulation" in the name of preventing or repressing abuses of freedom of expression and communication. These calls could materialize by increasing the liability of host and access providers regarding the content that they either store or transmit.

For instance, UK members of Parliament have recently taken position against the "mere conduit" principle enshrined in article 12 of the directive, which ensures that the role of network operators and Internet access providers is limited to the transport of data. In April 2010, Jeremy Hunt, then conservative spokesman on culture, said that IAPs should take responsibility for copyrighted content and cooperate with rights holders, stating: "*I don't think it is satisfactory to say they are a 'mere conduit*"[18].

During the negotiations of the Anti-Counterfeiting Trade Agreement (ACTA), some negotiators also proposed that the liability exemptions of Internet service providers would be conditioned on an online service provider "*monitoring its services or affirmatively seeking facts indicating that infringing activity is occurring*"[19].

The Gallo report on the enforcement of intellectual property adopted by the European Parliament on September 22nd, 2010 also contains provisions calling for private copyright police, whereby enforcement would be achieved through extra-legislative and extra-judicial measures, upon mere accusations by the rights holders and with the cooperation of the Internet service providers[20]. Often mentioned in the field of online copyright infringement as a way to bypass the legal shield enjoyed by Internet technical intermediaries, such non-legislative measures could fundamentally alter the online ecosystem and undermine fundamental freedoms.

**Recommendation 5:**

In our view, the revision of the directive must put an end to this trend toward an increased liability of Internet service providers.

- Instead, the directive should affirm the principle that there should be a presumption of legality on all uploaded content.

17 La Quadrature du Net, February 25th, 2010, "*Spanish Presidency leading Europe towards Digital Inquisition?*'. *laquadrature.net*. Address: http://www.laquadrature.net/en/spanish-presidency-towards-digital-inquisition

18 Horten Monica, "Conservatives want to get rid of mere conduit ", *Iptegrity.com*. Address: http://www.iptegrity.com/index.php?option=com_content&task=view&id=508&Itemid=9

19 See page 28 of the version dated January 18th, 2010 of the draft ACTA : http://www.laquadrature.net/wiki/ACTA_20100118_version_consolidated_text#Page_28
"*New Zealand can, however, support the inclusion of a provision aimed at preventing a party to ACTA conditioning safe harbours on an online service provider "monitoring its services or affirmatively seeking facts indicating that infringing activity is occurring*".

20 The report calls for "*additional non-legislative measures are useful to improve the enforcement of IPR, particularly measures arising from in-depth dialogue among all those active in the sector*". See https://lqdn.co-ment.com/text/Gq4N8gUR9UB/view/

- In particular, in order to strengthen the principle enshrined in article 15, the directive should ban all types of mandatory preventive mechanisms aimed at preventing the publication of certain types of online content, whether these are imposed by administrative or judicial authorities. Article 12's "mere conduit" principle needs to be strongly reaffirmed.

**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?**

"Specific filtering" seems to refer to instances where specific Web content is targeted and filtered by a technical intermediary (specific filtering is therefore opposed to general, a priori filtering). Such systems, whether they are specific or general in their implementation, are not only technically ineffective but also totally disproportionate and dangerous.

Filtering, when carried on by telecoms operators, consists in monitoring Internet traffic and blocking certain types of data streams. Such practices can only give the illusion of actually repressing the offenses which they are supposed to tackle. Instances of filtering of images and movies of child abuse content has proven the many flaws of this enforcement method. The proponents of such schemes generally give two justifications. On the one hand, filtering is supposed to prevent people from inadvertently accessing such content while browsing the Web. On the other hand, it also aims at tackling the voluntary access to such content by people . In the extremely theoretical case of inadvertent access[21], filtering software installed by Internet users on their computers would be much more effective and less intrusive than networked-based filtering. In the case of voluntary access to illegal material, the existence of numerous circumvention techniques makes filtering totally ineffective. Filtering only seeks to address distribution techniques that were used in the first years of the Internet but that have since then given way to much more sophisticated methods. The latter were developed with the aim to make sure that the business of the various criminal organizations engaging in the commerce of child abuse content would not be hampered by the development of Internet filtering. Consequently, they have developed invisible hosting networks distinct from the public Internet and which are totally impermeable to filtering techniques[22]. The spokesperson of the Internet Watch Foundation, which maintains the list of the websites filtered by UK Internet access providers, admits that Net filtering is only effective to block inadvertent access, for which much less intrusive and more effective tools already exist, as mentioned above[23]. Filtering is not only ineffective in the case of pedopornography. Even non-professional websites can readily circumvent to remain available online. For instance, an antisemitic website Aaargh, which is supposed to be blocked by French access providers following a court order[24], is still easily accessible online to all Internet users.

Also, Internet filtering can be counterproductive. Researchers Tyler Moore and Richard Clayton have show that the national implementation of Internet filtering to fight online child abuse have disincentivized the international cooperation between jurisdictions aimed at investigating and

21 The reality and frequency of such inadvertent access will still have to be demonstrated, since such67 material are usually hidden in "dark" areas of the Web, as pointed out below.

22 See Fabrice Epelboin, 2010, "Le commerce de la pédopornographie sur Internet de 2000 à 2010". Address : *http://bit.ly/pedobiz*

23 BBC, May 29th, 2010http://news.bbc.co.uk/2/hi/technology/8596650.stm, "Delete child abuse websites says German minister". Address :

24 Aaargh case. Decision n° 707 of June, 19th, 2008. Cour de cassation, first civil chamber. http://www.courdecassation.fr/jurisprudence_2/premiere_chambre_civile_568/arret_no_11682.html

repressing the production and distribution of pedopornographic content[25]. Such cooperation has so far been lacking at the European level, where the UK, France and the former German government have opposed the creation of a centralized service pooling the efforts of member states in the fight against child pornography. Too little is done to remove such offensive content and investigate on the criminal organizations who abuse children, which by far the most effective method to fight against this plague. Filtering only gives the illusion of tackling this pressing issue, while actually detracting us from the only truly adequate solution.

Lastly, Internet filtering is also dangerously inaccurate and leads to the over-blocking of perfectly legitimate online content[26], as exemplified by the case of the blocking of Wikipedia by British ISPs in late 2008[27].

Beyond the category of child pornography, there have been numerous cases across Europe where courts or lawmakers have imposed filtering obligations. For instance, in 2008, in the Aaargh case mentioned above, the French Court of Cassation confirmed a court order forcing all Internet Access Providers operating in the country to block access to an antisemitic website hosted in the United States. In a similar ruling, the August 2010 online gambling law let to a decision in which a judge ordered French IAPs to block access to a website hosted in the United Kingdom, explicitly referring to various Internet blocking methods, such as Deep Packet Inspection, that are very controversial for of their adverse effects on privacy[28].

The obvious ineffectiveness of filtering schemes and the risk of suppressing perfectly legal online speech make this enforcement method a disproportionate measure. From a legal point of view, since it is either ineffective or other methods are available to meet the same objective, it appears that filtering should be disqualified as a mode of law enforcement. When it is put in practice, only a judge should be able to order such a measure, after a thorough proportionality test[29].

**Recommendation 6:** The development of filtering amounts to building a technical infrastructure allowing for the largely automated censoring of information flowing through the Internet architecture. What is the most worrying is that our liberal democracies are currently adopting such method in spite of this ineffectiveness and the dangers these measures.

- In our view, because of the technical defaults of filtering measures, the directive could

25 Moore Tyler and Clayton Richard, 2008, "The Impact of Incentives on Notice and Take-down", Computer Laboratory, University of Cambridge. Address : http://www.cl.cam.ac.uk/~rnc1/takedown.pdf

26 As recognized by the French government itself in its impact assessment of LOPPSI. http://www.ecrans.fr/IMG/pdf/pl1697.pdf

27 *Wikinews*, 7 December 2008, "British ISPs restrict access to Wikipedia amid child pornography allegations". Address : http://en.wikinews.org/wiki/British_ISPs_restrict_access_to_Wikipedia_amid_child_pornograp

28 Béjot Michel and Bouvier Caroline, 2010, « France: Gambling and Betting on the Internet: French Courts Steps In and Requires the Service Providers to Block an Illicit Website », Address : http://www.gala-marketlaw.com/joomla4/index.php?option=com_content&view=article&id=291&Itemid=182

29 For more information on the exclusive competence of the judiciary to infringe on people's freedom of communication online, see Callanan Cormac, Gercke Marco, De Marco Estelle and Dries-Ziekenheiner Hein, 2009, "Internet Blocking: Balancing Cybercrime Responses in Democratic Societies", Aconite Internet Solutions. Address: http://www.aconite.com/blocking/study
See also La Quadrature du Net's memo in defense of "Amendment 138", which argues for the principle that any restrictions to Internet access, in that they prevent the practical exercise of freedom of expression and communication and in order to ensure the proportionality of any such restriction, should only be imposed subsequently to a decision by the judicial authorities. Address: http://www.laquadrature.net/en/legalese-for-progress-not-political-weakness

usefully be amended to ban injunctions leading to Internet traffic filtering.

- At the very least, the directive must specify that if member States decide to adopt Internet filtering measures, they should only used as a last resort, in cases where the removal of online content is impossible. Moreover, these measures should be pronounced after a due process before an independent and impartial court, after a sound proportionality assessment, ensuring that they are both effective and the least restrictive alternative (the court may find that these measures are unworkable, ineffective, that other less intrusive measures are better suited and determine that the proportionality criteria cannot be met).

**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?**

The introduction of technical standards for filtering at the European level would not do anything to remedy to the ineffectiveness of filtering measures. Whether they are network or content-based, filtering schemes suffer from their inability to correctly assess the legal situations they are supposed to apprehend. This is typically the case in the realm of copyright, where the transmission of a copyrighted works over networks does not in and of itself amount to an infringement. In many cases, such transmission will be totally lawful under the various exceptions and limitations to copyright provided by law (for purposes of quotation, information or private copying, for instance). Preventive filtering systems, such as YouTube's content ID[30], are unable to correctly assess whether a given use of copyrighted material constitutes an infringement. For more legal certainty, the filter will consider all the files that include such copyrighted works as unlawful, and will remove the latter.

Prevention of publication through automatic systems is bound to impede legitimate acts such as parody, presentation for the sake of information and criticism or the right of quotation. If such systems are given any legal status or even a simple recognition, there is a high risk that powerful right holders will use them as anti-competitive tools.

Filtering and other technical means of law enforcement in the digital environment also carry the significant risk of indirectly promoting the both the circumvention of these measures as well as the encryption of Internet communications. In the context of the debates on three strikes laws aimed at tackling online file-sharing in the UK and in France, the secret services of the United States and the United Kingdom have voiced their concern[31]. They fear that these repressive schemes will drive a large number of people to switch to using encrypted Internet tools, making it much more difficult to carry on their duty. Filtering will likely have similar consequences.

Unfortunately, in the name of the protection of a copyright regime profoundly at odd with digital technologies, the principles embedded in the liability exemptions provided by the e-Commerce directive are progressively eroded. As DeBeer and Clemmer explain:

30 http://www.youtube.com/t/contentid

31 See TechDirt, March 15th, 2010, "BPI Says That UK Spies Are Against Digital Economy Bill". Address: http://www.techdirt.com/articles/20100315/0034508554.shtml

TechDirt, October 6th, 2010, "US Intelligence Agencies Angry At France Over Three Strikes; Worried It Will Drive Encryption Usage". Address: http://www.techdirt.com/articles/20101006/04135311311/us-intelligence-agencies-angry-at-france-over-three-strikes-worried-it-will-drive-encryption-usage.shtml%29

> *"Previously, the worldwide standard approach to issues of Internet service provider liability was to require carriers and hosts to behave passively until becoming aware of copyright-infringing activities on their networks (...). Very recent events in several jurisdictions demonstrate a new trend away from a passive-reactive approach toward an active-preventative approach instead.*
>
> *Government policies, voluntary practices, legislative enactments, and judicial rulings are all contributing to this shift in the rules applicable to online intermediaries. One reason for the shift is increased pressure from rights holders on legislators and policymakers to make intermediaries play a greater role in online copyright enforcement. Another less obvious reason is that intermediaries' and rights-holders' interests are aligning. While rights holders are concerned about copyright enforcement and intermediaries are concerned about network management, the result is a mutual interest in content filtering or traffic shaping."*[32]

In Europe, this trend is exemplified by numerous initiatives taken by the Commission[33], or by the European Parliament through the adoption of the Gallo report on the enforcement of intellectual property, which focuses to a great extent on file-sharing. Instead, the EU must oppose these trends towards a turning technical intermediary into a copyright Internet police.

**Recommendation 7:** In spite of this worrying trend, it is clear that the promotion of technical standards for filtering at the EU level would only make the matter worse for law enforcement, by pushing users towards circumvention of filtering schemes as well as encryption of their Internet communications, with no proven benefits for the music and movie industries or authors and artists. Consequently, European lawmakers should reject filtering as an effective and sound public-policy to the challenges of online law enforcement.

**62 What is your experience with the liability regimes for hyperlinks in the Member States?**
**63 What is your experience with the liability regimes for search engines in the Member States?**

Although a few member States have developed special liability regimes for information location tools such as hyperlinks and search engines, EU law remains silent on the matter. The development of diverging case law on the matter should compel EU lawmakers to enact provisions harmonizing the liability regime applicable to such information location tools.

**Hyperlinks.** The World Wide Web has turned the Internet in a global and integrated public sphere, drawing new audiences able to use the unrivaled means of communications. Largely based on outgoing and incoming links, the Web relies on hyperlinks as way to quote content hosted by third-parties. The right of quotation being essential to the functioning of the online public sphere, and since it is unreasonable to expect someone who created an hyperlink to be responsible of the content presented on a linked Web page since the content might change over time, hyperlinks

32 DeBeer Jeremy F. and Clemmer Christopher D., *op. cit*.
33 See the various initiatives:
- DG Internal Market Dialogue on illegal uploading and downloading;
- DG Internal Market dialogue on "sale of counterfeit goods on the Internet"
- DG Home Affairs Dialogue on public-private cooperation to counter the dissemination of illegal content in the European Union.
- DG Home funding for "self-regulatory" Internet blocking.

providers should enjoy a liability exemption similar to that of host providers.

**Search Engines.** Search engines operate as a technical tool automatically indexing Web pages and offering users a spectrum of hyperlinks leading to online content matching desired key words. They perform a task of "merely technical and automatic nature"[34]. They should also benefit from liability exemptions, as several member States have recognized.

**Recommendation 8:** The liability regime of information tool providers should be harmonized at the EU level.

- The right of quotation being essential to the functioning of the online public sphere, and since it is unreasonable to expect someone who created an hyperlink to be responsible of the content presented on a linked Web page since the content might change over time, it seems that hyperlinks providers should enjoy a liability exemption similar to that of host providers.

– Search engines should also benefit from the liability exemptions guaranteed to host providers, granted that they are give transparent information regarding the way the information presented is automatically selected, ranked an prioritized, and whether and how certain types of information might be removed from the search results.

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

Regarding participatory websites which include spaces open to the contribution of all Internet users (such as blogs, discussion forums, websites open to users' comments), there seem to be uncertainties regarding whether they can enjoy the liability exemptions provided for technical intermediaries in the e-Commerce directive. As a consequence, some courts still consider the operators of such websites to be the publishers of all the information available through their online services[35]. There are thus deemed liable for the content posted by their users, even when such content has not been moderated. Since June 2009, French law provides publishers of participatory websites with a new liability exemption inspired by the regime applicable to technical intermediaries:

> *"When the infraction results from the content of a message sent by a user to a public on line communication service and made publicly available by this service in a space for personal contributions identified as such, the director or co-director of publication is not liable as principal author if it is established that he had no knowledge of the said message before it was posted online or if, from the moment when he became aware of it, he acted promptly to remove this message"*[36]

34 Recital (42): "*The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored*".

35 See the Fillipis case in France, involving the website of the French newspaper Libération. Journaliste et "pire que la racaille" - LeMonde.fr, Address: http://www.lemonde.fr/societe/article/2008/11/29/journaliste-et-pire-que-la-racaille_1124889_3224.html

36 Article 93-3 of law 82-652 of 29 July 1982 on audiovisual communication as modified by article 27 of HADOPI law. The unofficial translation of the law is available at :

**Recommendation 9:** Online service providers hosting participatory spaces and non-professional publishers such as bloggers could greatly benefit from the creation of liability exemptions for user-generated content in EU law. They will provide them with more legal certainty regarding the possible legal consequences of opening their services to the participation of all, and therefore have the potential to encourage freedom of expression online. The e-Commerce directive should be amended to provide those hosting participatory spaces with a similar liability exemption.

**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. 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?**

No. This concept is so far only present in recital 42 of the directive, and the application of the directive show that there is still a lot of uncertainty around this concept, in spite of the ECJ ruling.

The revision of the e-Commerce directive should be the opportunity to decline this principle for the different activities carried on by the various technical intermediaries operating online (see question 62, 63, 64 and 68).

**Question 67**

Question 67 was answered along with question 58.

**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, there have been very dangerous confusions regarding the “hosting” classification. In France, in particular, technical intermediaries not playing any editorial role in the publication of online content have been qualified as “'publishers” by judges, automatically triggering a higher level of liability and causing unfortunate legal uncertainty on providers.

In 2007, social network MySpace was said to be a publisher by a Parisian court in the Lafesse Case[37]. The latter held that since MySpace allows users to upload content through a specific frame structure, and considering that it displayed an advertisement every time the video was viewed, MySpace could not enjoy the liability exemption granted to host providers[38].

Even more worrying is the fact that, in a January 2010 decision regarding copyright infringing reproductions of comics[39], the Court of Cassation itself ruled that host provider Tiscali

http://www.laquadrature.net/wiki/HADOPI_full_translation#Article_27

37 Tribunal de Grande Instance, Lafesse v. MySpace, June 22, 2007
Address: http://www.foruminternet.org/telechargement/documents/tgi-par20070622.pdf

38 DeBeer Jeremy F. and Clemmer Christopher D., *op. cit.*, p. 397.

39 Court de Cassation, Tiscali v. Dargaud, January 14th, 2010.

was a publisher because of the advertising displayed on the website.[40] In both rulings, service providers were considered to be publishers because they automatically showed advertising on their users' websites, which contradicts the principles of the liability exemptions provided to technical intermediaries by the e-Commerce directive.

Also in 2007, a following a dissimilar reasoning, the court ruled that video host provider Dailymotion was liable for the content [41]. The court held that Dalymotion had deliberately enabled mass-scale piracy, writing that "*it could not seriously be argued that the aim of the architecture and the technical means put in place by Dailymotion were merely meant to enable [any Internet user] to share their home-made videos with their friends or the wider Internet community.*" Dailymotion was liable, since the Court took the view that exemption from a general duty to monitor their network "did not apply when the unlawful activities were generated or induced by the service provider itself". Shortly thereafter, Dailymotion implemented a filtering system screening users' uploaded content to detect copyrighted material.

This latter ruling shows that rather than establishing a coherent case law, French courts have qualified differently almost identical technical activities (see Lafesse and Nord-Ouest Prod. Cases). In all three cases, even in the absence of any editorial activity on the part of the service providers, judges have sided with the plaintiffs and condemned innovative online service providers when a common sense understanding of the principles embedded in EU law would have led to qualifying them as host providers.

**Recommendation 10:** This alarming case law demonstrates that the e-Commerce directive is not detailed enough, and that the definition of host provider needs to be extended to cover all situations where the technical intermediary has exerted no editorial function regarding the allegedly illegal information on a given Web page[42].

We believe that the ECJ ruling in the LVMH case mentioned above, which quotes the directive's recital 42, comforts this approach. As with participatory websites and search engines, the directive articles must guarantee that the liability exemptions apply in all cases where the illegal information (as opposed other content presented on the same Web page) was made available through a "merely technical and automatic" action by the service provider.

**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.**

Far from suffering from a lack of investment in law enforcement, the fifteen-year-long fight against file-sharing has led to countless laws and court actions, thereby mobilizing enormous resources. Regarding non-profit sharing of cultural works of the Internet, we don't think there is such thing as "piracy problem". *If* it is true that some sectors in the industry suffer losses because of file-sharing, then the money is simply transferred to other activities[43] that are probably more useful

Address: http://www.droit-technologie.org/upload/actuality/doc/1294-1.pdf

40 Vandevelde Bertrand, January 25th 2010, *Affaire Tiscali*, Address : http://www.droit-technologie.org/actuality-1294/responsabilite-des-hebergeurs-affaire-tiscali-la-cour-de-cassation.html.

41 Tribunal de Grande Instance, Nord-Ouest Prod. v. S.A. Dailymotion, July 13, 2007 http://www.juriscom.net/documents/tgiparis20070713.pdf

42 In the Tiscali case, the ads were automatically processes, and the infringing content posted by the user.

43 Live performance, video games, hardware, Internet and other telecommunications subscriptions, etc.

for EU economic and social wealth. But now, dozens of independent studies[44] – including from the OECD, IPSOS, the Canadian Department of Industry and other academics as well as governmental sources – show a neutral or positive economic impact of file-sharing on the creative sector.

The "problem" is that today's copyright regime is by far too rigid and is in practice profoundly at odds with the digital environment. If our societies are to fully benefit from the Internet, lawmakers need to move away from brutal enforcement of outdated and restrictive "intellectual property" regimes and demonstrate pragmatism. In particular, one fundamental fact needs to be acknowledged by policy-makers and cultural businesses alike: digital technologies allow for the perfect replication of cultural goods at virtually no cost. Regulations that run counter to this reality – for example by trying to alter the architecture of the Internet in order to deter copyright infringements, or by imposing technical measures that artificially recreate the scarcity that existed in the "old" cultural economy – defy common sense and hold back socio-economic progress while being often unrealistic from a technical point of view, as we have outlined in our answers to the previous questions.

**Recommendation 11:** EU lawmakers should instead reorganize the Internet-based creative economy around the emancipatory practices enabled by new technologies, such as the sharing and re-use of creative works. These practices promise a participatory culture where people can not only access, share and comment the works of others, but also use new tools to express their own. It also serves a bottom-up innovation process whereby new usages arise, generating economic growth and new social practices. If the European Union adapts copyright law in accordance with new technologies, a vibrant and innovative commercial cultural economy can develop along with other financing schemes to support this new creative ecosystem and provide appropriate monetary rewards for creators. Society as a whole would benefit from a new-found balance between the rights of the public and the interests of authors and producers. Otherwise, copyright will face a disastrous legitimacy crisis.

For more detailed proposals on how copyright needs to be reformed, see our response to the creative content consultation: http://www.laquadrature.net/files/LaQuadratureduNet-20100105Online_Creative_Content_Consultation.pdf

44 A compilation of such independant studies: http://www.laquadrature.net/wiki/Studies_on_file_sharing_eng