IRIS plus
LEGAL OBSERVATIONS
OF THE EUROPEAN AUDIOVISUAL OBSERVATORY

Filtering the Internet for Copyrighted Content in Europe

by Christina Angelopoulos

EDITORIAL

One issue that has been frequently discussed in the IRIS *plus* series is the unauthorised supply of copyright protected works via the Internet. The resulting threat of copyright infringements could, at least partly, be prevented through the use of Internet filters, an option that forms the subject of this latest edition of IRIS *plus*.

The article considers, among other things, which services (simple hosting or Internet services?) Internet filters are useful for and where they are therefore commonly used. This inevitably leads to the question whether such filters should be used voluntarily or made compulsory by law or a court order. Referring to several recent court decisions, Christina Angelopoulos demonstrates that answering this question can quickly become a balancing act between a law-based reaction to actual infringements on the one hand and a potentially unlawful general obligation to monitor content on the other. This throws up the fundamental question of the extent to which the human right to freedom of information is or should be limited by Internet filters.

The relationship between the E-Commerce Directive on the one hand and the Copyright Directive on the other is also central to determining under what conditions and for what content the use of Internet filters can, if necessary, be enforced. The revision of the E-Commerce Directive is bound to influence the future of Internet filters. The author suggests how things might develop, including the possibility of self-regulation, some examples of which are mentioned in this IRIS *plus*.

Strasbourg, March 2009

Susanne Nikoltchev
IRIS Coordinator
Head of the Department for Legal Information
European Audiovisual Observatory

IRIS *plus* is a supplement to **IRIS,** *Legal Observations of the European Audiovisual Observatory,* **Issue 2009-4**

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

76 ALLEE DE LA ROBERTSAU • F-67000 STRASBOURG
TEL. +33 (0)3 88 14 44 00 • FAX +33 (0)3 88 14 44 19
http://www.obs.coe.int
e-mail: obs@obs.coe.int

IRIS plus
LEGAL OBSERVATIONS
OF THE EUROPEAN AUDIOVISUAL OBSERVATORY

Filtering the Internet for Copyrighted Content in Europe

Christina Angelopoulos
Institute for Information Law (IViR), University of Amsterdam

Introduction

Over the past decade, Internet filters have stepped into the limelight. Heralded for their promise of control over the erratic diversity of cyberspace, filters are increasingly promoted as the most efficient way to combat phenomena as disparate as child pornography, online gambling, Internet security breaches and copyright infringement.[1] Yet, the feasibility and appropriateness of such plans have been brought into question, with many insisting that contemporary filters are neither sensitive nor intelligent enough to correctly categorise the content they encounter.[2] However, an analysis of the technological capabilities of modern filter software is beyond the scope of this IRIS *plus*. Instead, below, the legality of filter use shall be approached under the assumption that filters are capable of correctly distinguishing legal from illegal audiovisual content. Upon this premise, the current European legislative framework shall be analysed so as to detect by whom and under which conditions the use of filters may be required in the EU for the removal or prevention of access to copyright protected audiovisual content. In this context, the rules governing the liability of the online intermediaries, on whose networks and websites copyright-defending filters would be applied, shall first be examined, along with their interpretation by recent EU Member State case law. The text shall then turn to the limits set to filter use by freedom of expression concerns, in view of Article 10 of the European Convention of Human Rights (ECHR) and in the context of the recent Council of Europe (CoE) Recommendation on Internet filters. Finally, focus will turn to the current voluntary (in the sense of both self- and co-regulatory) uptake of filtering by Internet intermediaries.

1. The Existing European Legal Framework Governing Filtering

In principle, anyone who contributes directly or indirectly to the violation of an exclusive right may be held liable for copyright infringement. An exception is introduced in the area of online intermediary liability by the establishment in Europe of a separate regulatory framework for so-called "information society services", when acting as intermediaries. The E-Commerce Directive[3] contains a cluster of horizontal conditional liability exemptions, or "safe harbour" provisions, for certain activities or functions performed by online intermediaries, namely "mere conduit" (Article 12), "caching" (Article 13) and "hosting" (Article 14). Each safe harbour is governed by a separate set of conditions that must be met before the intermediary may benefit. In addition, Article 15 of the Directive prohibits the imposition of general obligations on such service providers to monitor the information which they transmit or store or to actively seek facts or circumstances indicating illegal activity. Below, we shall concentrate on filtering on the level of websites and Internet access providers (IAPs), these corresponding to the E-Commerce intermediaries providing hosting and mere conduit services.

What does the above-mentioned limited liability regime imply for the state-ordered application of filtering technology for the protection of copyrighted content? In general, the term filtering may be said to apply to content-control software applications designed to automatically block the display or downloading of selected material on a web browser or other Internet application[4]. This can be achieved through a variety of different technical methods: among others, as shall be seen below, a simple filtering strategy involves the blocking of content on the basis of the IP-address or URL at which it is located. Such an approach, which is achieved through a human decision to blacklist specifically targeted material, does not engage Article 15 of the E-Commerce Directive. On the other hand, the new generation of increasingly sophisticated filtering tools is harder to reconcile with a ban on the imposition of general monitoring obligations.[5] An example of such a tool would be the popular fingerprinting technology developed by companies such as the technology and services corporation Audible Magic: fingerprinting technology uses a unique digital representation of each piece of protected content, *e.g.* of a video-clip (a "fingerprint" of the content) to identify it

among all the traffic uploaded on a hosting website or flowing through a network, by means of comparison with a pre-existing extensive reference database of all fingerprints collected. Rightsholders who want to protect their work online can contribute a fingerprint of that work to the database.[6] If a match is detected, blocking ensues. The advantage of fingerprinting technology over IP blocking is that the detection of unwanted material is automated, while the disadvantage, from a legal point of view, is that it involves the monitoring of the totality of the information passing through an Internet service provider (ISP).[7] In the United States, the Digital Millennium Copyright Act explicitly stipulates that in order to be eligible for the corresponding liability limitations introduced in its text, service providers have to accommodate and not interfere with standard technical measures that enable copyright owners to identify and protect their work, to the extent that they do not impose substantial costs on the provider or burdens on their system or networks.[8] By contrast, no such caveat exists under European legislation, initially leading commentators to conclude that the EU's "harbours" were completely "safe" from filtering technology – the Article 15 preclusion of a general duty to monitor is absolute.[9] Nevertheless, this view has come up against a number of stumbling blocks over the past few years, as courts have appeared reluctant to grant online intermediaries full liability exemption for failure to filter. Furthermore, the safe harbours are only designed to protect ISPs from liability for monetary relief – injunctions may still be imposed for the prevention of copyright infringement. A selection of case law exhibiting the various tactics adopted to impose a greater degree of scrutiny on these services is examined below. The first set of cases deals with attempts to find ISP liability for neglecting to use filtering tools, while the second set deals with court injunctions obliging ISPs to do so.

1.1. Intermediary Liability and Filtering Obligations

A. The MySpace Case

In June 2007, the French *Tribunal de Grande Instance de Paris* (Paris High Court of First Instance – *TGI Paris*) denied the online social networking site MySpace classification as a hosting service (*hébergeur*), thereby disqualifying it for the application of the Article 14 liability exemption.[10] According to the court, the imposition of a pre-designed page set-up for users' personal accounts, in combination with the revenue-generating advertisements exhibited upon each visit, established MySpace's status as a publisher of content (*éditeur*). Similar decisions have been issued by French courts in the past.[11] Seeing as the liability regime for publishers is significantly stricter than that applicable to host providers, by classifying MySpace as a publisher, the ruling effectively encourages the site to utilise automatic filtering systems, so that the posting of infringing material that could compromise its legal position is avoided. If an information society service cannot benefit from any of the E-Commerce Directive safe harbours, it will be subject to national copyright legislation outlining the requirements for direct or indirect infringement and the defences available.[12]

B. The Dailymotion Case

In early 2007, upon the discovery of unlawful copies of the film "Joyeux Noël" hosted on the User-Generated Content (UGC) video-sharing platform "Dailymotion", the producer, director and distributor of the film initiated a lawsuit against the website for copyright infringement.[13] This time, the plaintiffs' claim that Dailymotion functioned as a publisher was rejected – instead, in a decision issued in July 2007, the TGI Paris found that Dailymotion's advertising-based business model does not detract from the fact that the content is uploaded by users, thereby qualifying Dailymotion as a hosting provider.[14] Having said this, the court then stated that Article 6-I-2 of the *Loi pour la confiance dans l'économie numérique* (Act on Confidence in the Digital Economy – LCEN[15]), which implements Article 14 of the E-Commerce Directive, does not provide an exemption from liability, but only a limitation. It then went on to hold that the architecture and technical means put in place by Dailymotion enabled illicit activities, while the very success of the website depended on the making available of copyright-protected material by its users. Given that Article 6-I-2 LCEN requires that, in order to claim protection from liability, a hosting provider must (a) not have had actual knowledge of illegal activity or of facts or circumstances that render such activity apparent; and (b) upon obtaining such knowledge, have acted expeditiously to remove or disable access, Dailymotion was considered ineligible for the application of the safe harbour provision. It should be noted that these conditions only concern hosting providers and not mere conduits or caching services. Dailymotion then recalled the proscription of a general obligation to monitor as imposed by Article 6-I-7 LCEN (implementation of Article 15 E-Commerce Directive). The court, however, rejected this reasoning, estimating that the prohibition only applies in cases where the unlawful activities were not generated or induced

by the intermediary itself. By contrast, the court held that intermediaries who provide their users with means for infringing copyright have a duty to carry out prior control for the prevention of such user behaviour. By abstaining from the implementation of equipment preventing access to the film, Dailymotion had breached this obligation. Accordingly, Dailymotion was found liable for copyright infringement and ordered to pay damages.

The ruling has given rise to debate and criticism, in particular surrounding the imposition of a novel duty upon service providers for an *a priori* implementation of technical filtering measures for the prevention of online piracy. The court's reasoning is especially puzzling given that the facts of the case reveal that Dailymotion had failed to withdraw all infringing videos from its site, even after notification on the part of the rightsholders – behaviour that would in any case normally have precluded the deployment of the Article 14 "hosting" safe harbour. In view of Dailymotion's breach of its reactive obligation to prevent infringements brought to its attention, the need to impose a proactive duty on hosting intermediaries to block all unlawful content is questionable and difficult to reconcile with Article 15 E-Commerce Directive. Indeed, in its strictest interpretation, the innovative obligation does away with most safe harbour benefits, effectively equating the liability of a hosting platform with that of a publisher.[16] The decision is currently under appeal.

C. The Tranquility Bay Case

In October 2007, the TGI Paris ruled that the UGC video-sharing service Google Video was liable for copyright infringement, due to the multiple unauthorised copies of the documentary "*Les enfants perdus de Tranquility Bay*" present on its website.[17] As in the Dailymotion case, the court again conceded that Google Video did qualify for the safe harbour extended to hosting services by Article 14 E-Commerce Directive. Moreover, the facts of the case revealed that this time the service provider acted expeditiously to disable access to the infringing copies of the film upon notification by the rightsholders. Nevertheless, each removal of the infringing content was followed by speedy re-postings, forcing the rightholders, website and users into a repetitive game of cat and mouse. The court concluded that, once Google had been informed of the existence of infringing copies of the film, it was under an obligation to implement any means necessary to avoid future dissemination; consequently, although the speedy blocking of access to the unlawful video upon the first notification exonerated Google on that single instance, Google failed to comply with the conditions of Article 6-I-2 LCEN in respect of every subsequent uploading. Google was therefore deemed to be liable.

Although crafted in more cautious terms than the preceding Dailymotion case – the imposition of a general duty of prior control over all copyrighted content uploaded by users onto the site is sidestepped[18] – the Tranquility Bay ruling likewise gives rise to questions of compatibility with Article 15 E-Commerce Directive. As commentators have observed, the TGI Paris likely rests its interpretation on Article 6-I-7 subparagraph 2 LCEN, which permits the imposition of specific "targeted and temporary" surveillance charges. Indeed, as the court reasons, although the multiple postings are attributable to different users, the content is identical, arguably rendering the monitoring obligation specific. However, Google was swift to take down all infringing copies tracked down through human observation on the part of the rightsholder. A duty to avoid future infringement (which was not observed) is difficult to reconcile with a ban on general monitoring by the intermediary. According to the interpretation of the court, if host service providers wish to avoid liability they are obliged, after receiving notification, to hunt out each and every remaining or reposted unauthorised copy, *i.e.* to practice general monitoring over all (even non-infringing) content on their website. In fact, as notifications are likely to accumulate at a fast rate, the only practical way to achieve this would necessitate the use of fingerprinting or similar automatic filtering technology. The specificity therefore of the obligation is negated by the broad reach of the ruling's implications, which affect the liability of all hosting services for all works for which a notification has been sent as to a single infringing copy. A safer approach, guaranteeing respect of the specific case requirement, would be the issue of an injunction imposing an *ex post* obligation to prevent infringements only in the specific instance under review (see below, Section 1.2), *e.g.* in this case, to prevent future infringements exclusively of "Tranquility Bay". In the present case, no such injunction had been issued; to the contrary, the court seems to be placing liability-expanding powers with *ex ante* effect in the hands of rightsholders, thereby enabling the suspension of the Article 14 hosting safe harbour upon rightsholder request and with no need for prior judicial review.[19]

As becomes apparent from the above analysis of the inconsistencies and clumsy evolution in the reasoning of

the case law even within a single member state, the courts would appear to be somewhat bewildered as to the correct application of the safe harbour provisions, while simultaneously groping through the new restricted legal framework for ways of imposing liability in the face of mass piracy and the difficulties in identifying and bringing to court the individual users responsible.[20]

1.2. Injunctive Relief and Filtering Obligations

The liability rules of the E-Commerce Directive are exclusively confined to claims for monetary relief by rightsholders against Internet intermediaries. The imposition of any kind of injunction by a court or administrative authority is expressly permitted by the final paragraph of each of the safe harbours of Articles 12-14, which provide the possibility for "courts and administrative authorities" to order providers of information society services to "terminate or prevent an infringement". Article 8(3) of the Copyright Directive[21] also explicitly instructs Member States to "ensure that rightsholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right", while the 2004 Enforcement Directive[22] reinforces this obligation in Article 9(1), which refers to the Copyright Directive and repeats the order. Yet, in the area of filtering, dovetailing this possibility with Article 15 of the E-Commerce Directive constitutes a difficult balancing exercise. The preamble to the E-Commerce Directive elucidates the permitted scope of such an order: injunctions may be imposed for the "prevention of any infringement, including the removal of illegal information or the disabling of access to it" (Recital 45), but may impose a monitoring obligation only in a "specific case" (Recital 47). Injunctions, therefore, requiring the use of technical filtering systems may lawfully be imposed on service providers, but only to the degree that specific people, websites or content are affected.[23]

A. The SABAM/ Tiscali Case

In a landmark case, the Belgian *Société d'Auteurs Belge – Belgische Auteurs Maatschappij* (Society of Authors, Composers and Publishers – *SABAM*), initiated proceedings against the Belgian IAP Scarlet (former Tiscali), alleging that it knowingly permitted the illegal downloading of SABAM's protected works through peer-to-peer file-sharing on its network. SABAM requested the imposition of an injunction obliging the IAP to take proactive measures so as to prevent the unauthorised exchange of protected material by its subscribers. The *Tribunal de Première Instance de Bruxelles* (Brussels Court of First Instance – *TPI* Brussels) enlisted the services of a technical expert so as to assess the feasibility of such measures and, in June 2007, ordered Scarlet to install the content management and identification fingerprint-based system developed by Audible Magic.[24] Scarlet was given six months within which to comply with the order, while a fine of EUR 2,500 would be imposed for each day of delay thereafter.

The court reasoned that, given that Recital 40 of the E-Commerce Directive declares that "the provisions of this Directive relating to liability should not preclude the development and effective operation, by the different interested parties, of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology", the proscription of a general obligation to monitor does not prevent the use of filtering tools. The problem with this reasoning is that Recital 40, taken in its totality, refers to "voluntary agreements" reached between all parties concerned, rather than judicial injunctions. This fact does not pose a conclusive obstacle however, in view of the fact that injunctions requiring the prevention of an infringement can lawfully be imposed according to Recital 45 of the Directive. Turning to Article 15 itself, the court categorically stated that the injunctive relief requested did not require Scarlet to "monitor" its network or "to actively seek facts or circumstances indicating illegal activity". This conclusion is up for debate and likely depends on the technology applied, as well as the instructions issued by the court. The TPI Brussels also concluded that, the filtering instruments being limited to the blocking of only certain, specific information, no general obligation to monitor is imposed. Again, this is a factual matter that will depend on the way in which the particular tool executes its filtering objectives. The court did not give any indications as to its reasoning on these questions, yet, as explained above, only with difficulty can the digital fingerprinting technology employed by Audible Magic be considered distinct from general monitoring activities.

It is worth mentioning that Scarlet was wary of the use of filtering methods, for fear of compromising its mere conduit status through the modification of information contained in its transmissions. This position was convincingly rejected by the court: indeed again Recital 40's express permission for the use of such technology, as well as Recital 45's permission of injunctions should suffice to exclude such an eventuality.

As widely expected, Scarlet appealed the decision. A hearing is scheduled for October 2009, while, in the meantime, the unfolding events have only served to make the issue increasingly convoluted: in October 2008,[25] Scarlet was provided with additional time, until the end of that month, to implement the measures necessary for eliminating infringements, after demonstrating that the use of Audible Magic filtering software on its system had proved technically unworkable. The TPI Brussels nevertheless held that it was not unreasonable to require of Scarlet that it make greater efforts to execute the injunction and the IAP was asked to examine other filtering options.[26]

B. The Pirate Bay Cases

In August 2008, the *Giudice Per le Indagini Preliminari* (Court for Preliminary Investigations) of Bergamo placed the Swedish BitTorrent tracker website "the Pirate Bay" under preventive seizure in the context of a criminal investigation against its owners for aiding and abetting illegal file-sharing. To this end, Italian IAPs were ordered to apply filtering mechanisms to block access to the site. In September, the decision was challenged and subsequently overturned: according to the Court of Bergamo,[27] a preventive seizure is a judicial tool that may apply to a specific commodity and is characterised by its *erga omnes* effects, so far as it results in a prohibition on anybody from using the object. In the case of a website based outside of national territory, the only way to achieve the same effect is through an order forcing national IAPs to block access to the website, yet, in this way, the nature of the measure is completely altered: from an *erga omnes* proscription it now becomes a personal injunction against online intermediaries, an effect only permissible under Italian law in specific *numerus clausus* cases, which do not include copyright infringement. The decision sits well with the above interpretation of the E-Commerce and Copyright Directives: injunctions may be issued by national authorities ordering monitoring obligations against online intermediaries benefiting from safe harbour provisions and nevertheless carrying a third party infringement of a protected work in their networks. These injunctions may include the removal of the illegal information or the disabling of access to it, but only in specific cases and in accordance with national legislation.[28]

This conclusion is oddly confirmed by a Danish decision which went precisely in the opposite direction: in November 2008, an appeal court in Denmark upheld a ruling ordering DMT2/Tele2, an IAP, to block access to the Pirate Bay. The Danish Sheriff's Court had earlier in the year[29] agreed that the IAP was exempted from liability in accordance with the E-Commerce Directive's liability limitation rules, but noted that nothing prevented the application of an injunction. Thus, the crucial question lay not in the safe harbour provisions, but in whether or not the conditions set out in Danish procedural law for the issue of an injunction were met. This was found to be the case: the court held that the Pirate Bay violated copyright law, while DMT2 contributed to the violation of copyright legislation performed by the Pirate Bay through the transmission via its networks of protected content. It also found that DMT2 independently infringed copyright due to the automatic, intermediate and transient storage of said content in the course of transmission. The Sheriff's Court held that the case could not await ordinary trial, while the imposition of an obligation upon DMT2 to block access was not evaluated as disproportionately harmful to the IAP. The reasoning in the ruling is in conformity with previous Danish Supreme court case law.[30]

1.3. Projected Legislative Amendments and Clarifications

Article 21 of the E-Commerce Directive enjoins the Commission to prepare a biannual report on the application of the Directive, accompanied, where necessary, by proposals for adapting it to legal, technical and economic developments. The launch of a public consultation to identify the shortcomings of the existing legal framework was imminent when this IRIS *plus* went to press. The consultation is intended to lead to a new report in the second half of 2009 and ultimately to a new legislative proposal.[31] In the new report, special attention will be paid to the question of intermediary liability and the monitoring role of ISPs.[32] It is to be hoped that the review will bring more clarity both to the issue of the correct method of employment of the three safe harbours[33] and to the appropriate approach to striking a balance between the Copyright and the E-Commerce Directives in the case of injunctions. If injunctions can be issued by the courts against intermediaries who carry third party copyright infringement pursuant to the Copyright Directive, can these injunctions constitute a general obligation to monitor, thereby compromising Article 15 of the E-Commerce Directive? If not, when can a monitoring obligation be said to be confined to a specific case within the meaning of the E-Commerce Directive and is the difference between an IAP and a hosting service relevant in this context? Does the use of filtering tools constitute general monitoring and if so, which of these tools are affected? These are all press-

ing questions, the answers to which cannot be expected to be provided by courts across the European Union in a coordinated manner without harmonising legislative or jurisprudential guidance.

Legislative adjustments or clarifications are underway in relation to other EU Directives as well: in late 2007, the first Commission report on the application of the Copyright Directive was published.[34] The European Parliament's (EP) response, known as the Medina Report,[35] is due to go to vote in March 2009. The latest draft, working upon the presumption that all peer-to-peer downloading is illegal, praises the blocking of the Pirate Bay on judicial order, encourages the launch of filtering technology and invites reflection on the question of ISP responsibility to fight against piracy. If adopted, the report will signal a marked EP turn-around from the attitude displayed in last spring's Bono Report,[36] in which amendments tabled to the effect of obliging ISPs to adopt filtering technologies were withdrawn from the final text.

In addition, the reform of the package of EU Directives regulating the European telecoms market ("Telecoms Package"),[37] might also prove consequential in this context. Amendment 112 (Article 33 2(a)) of the Harbour Report[38] is central, as it instructs national telecoms regulators to oversee "co-operation" between IAPs and rightsholders. Such co-operation could conceivably involve filtering.[39] To balance this out, the European Parliament introduced the controversial Amendments 166 of the Harbour Report and 138 of the Trautmann Report.[40] These state that users' rights to access content, services and applications may not be restricted in any way that infringes their fundamental rights, including freedom of expression, while restrictions must be proportionate and require a prior ruling by a judicial authority. Both amendments were subsequently discarded, the first in the Commission's amended proposals[41] and the second in the Council's political agreement, although, in the run-up to the second reading before the EP, their reintroduction is rumoured. Plenary vote is planned for 21 April 2009. If passed, the amendments will explicitly introduce freedom of expression in the main body of EU directives relevant to filtering next to the other counterbalancing considerations.

2. Balancing Filtering with Freedom of Expression

In a recent Recommendation,[42] the Committee of Ministers of the Council of Europe drew attention to the fact that the use of Internet filtering methods may constitute a restriction on freedom of expression and access to information in the online environment. Even in the absence of the above-mentioned Telecoms Package amendments, this fact is not lost on the EC Directives either: in Recital 9, the E-Commerce Directive instructs that "directives covering the supply of information society services must ensure that this activity may be engaged in freely in the light of [Article 10(1) ECHR[43]] subject only to the restrictions laid down in paragraph 2 of that Article", while the Copyright Directive is also intended to relate "to compliance with the fundamental principles of law and especially of [...] freedom of expression". The CoE Recommendation distinguishes between mandatory filtering imposed through state intervention and filtering by private actors.

Filtering resulting from state intervention must always meet the requirements of Article 10(2) ECHR, *i.e.* any filtering measures applied must be prescribed by law in the pursuit of one of the aims recognised as legitimate by Article 10 and be necessary in a democratic society. According to the guidelines issued in the Recommendation, in the context of filtering this means, among other things, that:

(a) Filtering may only be demanded for one of the reasons set out in Article 10. These include the protection of the rights of others, *ergo* also of copyright.[44] The underlying report to the Recommendation expressly explains that filtering may be utilised for the blocking of access to unlawfully disseminated copyrighted content.
(b) Nationwide general blocking or filtering may only be introduced by the state if the filtering concerns specific and clearly identifiable content, a competent national authority has taken a decision on its illegality and the decision may be reviewed by an independent and impartial tribunal or regulatory body.
(c) The effects of the filtering must be proportionate to the purpose of the restriction.[45] According to the Recommendation, this involves assessment of the filter both prior to and during the implementation, so as to exclude the unreasonable blocking of lawful content.

State intervention will exist not only in the case of action on behalf of public bodies that is directly attributable to the state, but also where private bodies act on the instruction of the state. This would include content-blocking by an ISP following a decision by a state authority, thus such decisions should adhere to the Recommendation's

guidelines. The guidelines would seem to tally with the analysis engaged in above of ISP liability for failure to apply filtering equipment to avoid copyright infringement on their networks, as well as of injunctions imposing such an obligation. So, the *ex ante* finding of an obligation for online intermediaries to carry out prior control, such as that which was found in the Dailymotion case, is probably of dubious legal reasoning *vis-à-vis* Article 10 ECHR. To the contrary, a court order, which can be challenged through the usual avenues of the judicial system, whereby an Internet access provider must implement filtering technology, as permitted by national law, so as to prevent access to a specific and clearly identifiable website, after a finding of illegality on the part of said website, as happened in the Danish *DMT2* case, complies with the requirements of the ECHR. The Council of Europe's 2003 Declaration on freedom of communication on the Internet, further confirms this conclusion by stating that "[p]rovided that the safeguards of Article 10, paragraph 2, of the Convention for the Protection of Human Rights and Fundamental Freedoms are respected, measures may be taken to enforce the removal of clearly identifiable Internet content or, alternatively, the blockage of access to it, if the competent national authorities have taken a provisional or final decision on its illegality."[46]

But it is not only the external balancing with freedom of expression that may set limits to copyright and thereby to the legitimate use of filters to prevent infringement. Internal mechanisms also exist within the body of copyright law itself that safeguard free speech through the doctrine of limitations and exceptions to copyright.[47] For EU member states, such possible limitations and exceptions are restrictively listed in Article 5 of the Copyright Directive. Recital 59 of the Directive provides that injunctions against online intermediaries should be available to rightsholders even when the acts carried out by the intermediary itself are exempted under Article 5 of the Directive – so, for example, the fact that a reproduction of protected material by an IAP was transient or incidental in the sense of Article 5(1) Copyright Directive, will not serve as sufficient defence against the order of an injunction. But what if the acts of the users themselves fall within the protected area of Article 5? In the SABAM case, Scarlet pointed out that "the licit character of a transmission is an inaccessible fact to any technology." Moreover, even putting aside the Article 5 limitations and exceptions, the exchange of cultural material online, through peer-to-peer websites or other means, may be permissible because the work itself is not protected by copyright (*e.g.* the originality criterion is not fulfilled or the work has fallen into the public domain) or has been placed under a licence. For these reasons, prior decision by a competent authority ascertaining the illegality of content is of heightened importance, ensuring that a human element exists in the decision-making process that leads to blocking. In the case of the prevention of access to entire sites, as happened with the Pirate Bay, such a decision also guarantees the proportionality of the inadvertent blocking of permissible, lawfully disseminated content with the objective pursued and, thus, its necessity in a democratic society. The existence of an effective and readily accessible post-filter means of recourse and remedy is essential for the same reason.

In addition to state interventions ordering automatic filtering of content, filtering products can also be voluntarily employed by both private and public actors with a view to restricting access to certain content. Such actors may include individuals, *e.g.* parents opting to install filtering tools on their Internet connection so as to protect their children from potentially harmful content, or private or public sector institutions, such as libraries, universities, schools or enterprises. This second category is the one most likely to be motivated by copyright concerns: for example, universities across the United States have turned to filters so as to minimise the amount of illegal file-sharing taking place on their networks.[48] Such filters may be installed at the level of the individual computer, on an institutional level, on the website level or on the level of the Internet access provider.[49] As noted in the working paper accompanying the Recommendation, filtering deployed voluntarily by private actors will not be directly subject to Article 10(2) ECHR. Nevertheless, given that the state, according to the case law of the European Court of Human Rights, is the "ultimate guarantor of pluralism", it will still be incumbent upon it to safeguard the principle of freedom of expression.[50]

The CoE Recommendation also contains a number of guidelines dealing with the correct voluntary use of filters. These encourage (a) the regular assessment and review of the effectiveness and proportionality of filters, (b) the provision of information on the existence of filtering measures and the reasons for their introduction, as well as guidance to users on the criteria according to which the filter operates and (c) co-operation with users with a view to improving transparency, effectiveness and proportionality in the use of filters. In addition, civil society is encouraged to follow developments in this area and ensure that users' freedom of expression is guaranteed.

Contemplation of recent trends in the sphere of filter application reveals the full import of this section of the Recommendation. Increasingly, private actors are turning towards technical systems of identification and regulation, either as the best defence against allegations of liability or in the context of compromise achieved with rightsholders and their representatives. In fact, the E-Commerce Directive itself attempts to stimulate initiatives of this kind: as stated above (Section 1.2.A), Recital 40 of the Directive encourages the adoption of voluntary agreements between stakeholders for the development of "rapid and reliable procedures for removing and disabling access to illegal information", while also noting that nothing in its text should be read as precluding the use of technical filtering systems.

3. The Trend towards Voluntary Filtering

Days after the TGI Paris decision in the *Joyeux Noël* case, Dailymotion announced the installation of Audible Magic fingerprinting technology on its website. In October 2007, "Signature", the video fingerprinting technology of the *Institut national de l'audiovisuel* (the French national television archive – INA*)* was also added to its filtering arsenal. As Dailymotion explained in a press-release, "[t]he use of filtering and fingerprinting technology is a core part of Dailymotion's strategy of being a content owner friendly video sharing site."[51] MySpace also uses Audible Magic to recognise illegally copied content on its website,[52] while Google has introduced filtering technology of its own design on its major video-exchange platform YouTube.[53] The adoption of filtering technology may serve as a defensive mechanism against accusations of liability, a pre-emptive strike against injunctions imposing filters and also as a show of good faith towards rightsholders with a view to entering into licensing deals. In this way, the first seeds are planted for an innovative UGC platform business model, whereby a legal version of the advertisement-attracting use of professional content criticised by the TGI Paris is explored: rightsholders provide fingerprints that limit the appearance of unauthorised copies of their work on the hosting website and simultaneously increase their exposure through the provision of legal content, while the intermediary draws in a wider audience and with it more advertising-derived revenue.[54] This is a far cry from the initial sceptical attitude of commentators towards Recital 40 of the E-Commerce Directive, which predicted no incentive for online intermediaries to willingly adopt technical systems of protection.[55] It also increases the need for a self-moderating behaviour on the part of the private sector that takes freedom of expression concerns into account, as encouraged by the CoE guidelines.

Beyond this "self-filtering" independently adopted by individual websites, the inter-industry voluntary agreements which the E-Commerce Directive advances are also beginning to emerge. In October 2007, major US film and TV studios and a number of UGC hosting websites signed a set of non-binding collaborative "Principles for User Generated Content Services", a major focus of which is constructive co-operation on the use of content identification and filtering technologies.[56] The Principles foresee the installation, before a set deadline, and regular update of state-of-the-art filtering tools on UGC platforms with the goal of eliminating infringing content. Rightsholders take on a corresponding obligation to provide reference material enriching the platforms' fingerprint databases, while also relinquishing the right to take the intermediaries to court should infringement nonetheless persist. Rightsholders likewise undertake not to attempt the disqualification of the intermediaries from safe-harbour status on the pretext of use of filtering technology. Although this is a self-regulatory document and no state involvement in the form of prior assessment by a state authority or subsequent judicial recourse is envisaged, the Principles resemble the guidelines for member states set out by the CoE Recommendation in that they foresee:

(a) guarantees aiming at the limitation of false positives. These include a general admonition to allow wholly original and authorised uploads and accommodate lawful limitations and exceptions to copyright, as well as procedural guarantees such as white lists of authorised licence-holders and an option for manual (human, although not judicial) review.
(b) a process for dealing with conflicting author claims for reference data and user claims of inappropriate blocking.

In this way, respect for the freedom of expression of both rightsholders and users is underscored.

The Principles have drawn criticism due to the abstention of Internet giants Google and Facebook. They have also been accused of backing intermediaries into a corner under the threat of litigation.[57] Seen from a similar angle, it is true that, as with the above-mentioned "self-filtering", intermediaries draw their main incentive for entering into such voluntary *quid pro quo* agreements from the prospect of litigation minimisation. In this way, inter-industry voluntary agreements provide ISPs with another kind of "safe harbour": when refuge is no longer certain in legislation, ISPs form their own shelter in self-regulation and adjusted "best practice" business strategies.[58]

Civil society has also been active in carving freedom of expression limits to filtering: a coalition of relevant US institutions dealing with freedom of expression have suggested a complementary set of "Fair Use Principles for User Generated Video Content."[59] These reiterate the need to incorporate protection of legitimate limitations and exceptions to copyright in any filtering software, with especial emphasis on transformative uses. They also underscore that "humans trump machines", meaning that filtering should not result in automatic removal, but in a probing process, involving notice sent to the user allowing him to dispute the claim of infringement. Along the same lines, informal means of review in the form of a "dolphin hotline" are also envisioned, whereby an "escape mechanism" for fair use "dolphins" caught in nets intended for infringing "tuna" is put in place. The principles are drafted on the basis of the US fair use tenet and can only have application within Europe to the extent that they agree with national copyright legislation.

All the above, however, only concern hosting providers. Initially, it appeared as though filtering on the level of the IAP was also likely to flourish – yet, the trend seems to be moving in a different direction. Filtering is indeed mentioned in the recent French and British Memoranda of Understanding (MoU): in November 2007, the French Anti-Piracy Commission presented the so-called "Olivennes Agreement",[60] the result of a three-way deal between the government, IAPs and rightsholders. The agreement requests the phasing-in of filtering technology on video-sharing platforms with the collaboration of music and audiovisual content-owners. Nevertheless, it is mainly concentrated on the establishment of the so-called *riposte graduée* or "graduated response",[61] whereby infringers are sent warning messages by a public authority, which if repeatedly ignored culminate in the enforcement of sanctions, such as the termination of Internet subscriptions. The patronage of the French government signifies that, as opposed to the afore-mentioned principles, this time legally binding authority is intended to attach. However, for the time being, the future of the legislation necessary to implement the agreement hangs on the outcome of debate at EU level on the final texts of the Telecoms Package.[62] In the meantime, in July 2008, on the basis of Recommendation 39 of the Gower's Review of Intellectual Property commissioned in 2005 by HM Treasury to review the British intellectual property framework,[63] the UK followed in the footprints of the French: a government-brokered MoU[64] was signed between major rightsholders, government departments and IAPs, which aims at reducing illegal online file-sharing through a co-regulatory approach. The MoU does mention filtering and suggests that signatories explore the option – yet, its main focus is again on the introduction of a graduated response system. Indeed, the accompanying consultation document[65] only mentions filtering under the heading of "Other Options to be Considered," should the preferred co-regulatory solution fail.

The graduated response scheme is proliferating: Italy also seems set to follow the "French model",[66] while, in January 2009, a ground-breaking settlement was reached in Ireland between content-owners and Irish Internet access provider Eircom. The music labels had initially instigated proceedings requesting that Eircom be forced to implement filtering technology on its networks. The settlement instead swung towards the implementation of graduated response.[67] Across the Atlantic, the Recording Industry Association of America (RIAA) is adopting a similar strategy, with the Motion Picture Association of America in all likelihood heading in the same direction.[68] An indication as to why this shift in tactics might be taking place is offered by the Creative Content Online public consultation launched by the European Commission: in their responses, stakeholders were often sceptical as to the technical feasibility of filtering general Internet traffic, while, at the same time, IAPs have been reluctant to install such software for fear of degrading their network services. Finally, the knowledge standard of Article 14 on hosting services does not appear in Article 12 on mere conduits and, given that the finding of liability for a failure to apply filtering equipment in the Dailymotion and Tranquility Bay cases depended on the restrictive interpretation of "apparent", even if correct, this reasoning cannot be replicated in the case of IAPs. Given that the dust has not yet settled as to the feasibility or legality of scalable, intelligent filtering technology, this adjustment is probably sensible. It is worth pointing out that the UK government has cautioned against impulsive legislative moves, while also predicting that filters "may well be part of any solution but they are unlikely to offer a panacea".[69]

Conclusion

The provisions of the E-Commerce Directive lend themselves to conflicting interpretations. The safe harbours ought to preclude findings of intermediary liability due to failure to filter, yet, controversial interpretations by the courts have given rise to a strict application of the knowledge requirement. Injunctions against intermediaries

requiring the use of filter software are on the rise, although their issue requires careful navigation round the inscrutable provisions of the preamble to the Directive. Yet, the contours of the permissibility of state-imposed filters, as they emerge from the Directive, mostly coincide with those drawn by freedom of expression considerations: filters may only be imposed in specific cases, so as to block content the illegality of which has been confirmed by a state authority and only where means of review are readily accessible. The directions issued by voluntary inter-industry codes of conduct follow the same lines. Yet, for the moment, the voluntary up-take of automatic filtering applications seems to be limited to the level of hosting websites. On the level of IAPs, current trends seem to be moving away from the filtering solution. Instead, "graduated response" is the catchphrase on everyone's lips. It would seem therefore that, although the future may indeed lie with filtering, for the moment, the present does not.

1) Deibert, R. et al., *Access Denied - The Practice and Policy of Global Internet Filtering*, (MIT Press, 2007) and Zittrain, J., *The Future of the Internet and How to Stop It* (Penguin Books, London 2008).
2) Cho, C., Feldman, A. and Heins, M., *Internet Filters – A Public Policy Report* (2nd ed., Brennan Center for Justice at NYU School of Law) 2006, available at: tinyurl.com/dneu22
3) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce), [2000] OJ L 178/1.
4) Council of Europe, *Report by the Group of Specialists on human rights in the information society (MC-S-IS) on the use and impact of technical filtering measures for various types of content in the online environment*, CM(2008)37 add, available at: tinyurl.com/adyzoz
5) Rossenhövel, C., *Peer-to-Peer Filters: Ready for Internet Prime Time?* (Internet Evolution), available at: tinyurl.com/64dp68
6) See Audible Magic Corporation's response to the European Commission's Creative Content Online Consultation, available at: tinyurl.com/3cw4mq ; U.S. House of Representatives, Committee on Science and Technology, *The Role of Technology in Reducing Illegal Filesharing: A University Perspective* (Hearing Charter, 5 June 2007), available at: tinyurl.com/cteczv and Horten, M., *Deep Packet Inspection, Copyright and the Telecoms Package*, available at: tinyurl.com/bvj6av
7) The Oxford English Dictionary defines the verb "to monitor" as "a. To check or regulate the technical quality of (a sound recording, radio transmission, television signal, etc.) without causing any interruption or disturbance; […] b. To listen to and report on (radio broadcasts, esp. from a foreign country). Also: to eavesdrop on (a telephone conversation). […] c. *gen.* To observe, supervise, or keep under review; to keep under observation; to measure or test at intervals, esp. for the purpose of regulation or control."
8) Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) § 512 (i).
9) Koelman, K.J., *Online Intermediary Liability*, in Hugenholtz, P.B., (ed.) *Copyright and Electronic Commerce - Legal Aspects of Electronic Copyright Management* (Information Law Series (no. 8), Kluwer Law International 2000) 34.
10) Jean Yves L. dit Lafesse v Myspace, Tribunal de Grande Instance de Paris, Ordonnance de référé, 22 June 2007, available at : tinyurl.com/bdpm3a . A subsequent decision of the court of appeal has since also been issued, however this deals mainly with procedural issues (see MySpace Inc v Jean-Yves L dit Lafesse, SARL L Anonyme, Monsieur Daniel L, Monsieur Hervé L, CA Paris, 29 October 2008, available at: tinyurl.com/dcgmpk).
11) Tiscali Media v Dargaud Lombard, Lucky Comics, Cour d'appel de Paris (4ème chambre, section A) decision of 7 June 2006, available at: tinyurl.com/b3hk7q
12) In France, for example, according to Article 42 of the *Loi du 29 juillet 1881 sur la liberté de la presse* (Act on Freedom of the Press of 29 July 1881), in principle, the publisher of printed matter or audiovisual content is held liable merely on the finding of an infringement, while, according to the cascading system used, the author of the infringing text may either be liable as an accomplice or, only in absence of a publisher, exclusively liable. The publisher is therefore required to prevent unlawful activity from occurring in the first place. These regulations have been applied to hosting providers even before the introduction of the E-Commerce Directive (see Estelle H. v Valentin L. et Daniel, Tribunal de grande instance de Paris, Ordonnance de référé of 9 June 1998, available at: tinyurl.com/bvkxmx).
13) Christian, C., Nord Ouest Production v Dailymotion, UGC Images, *Tribunal de Grande Instance de Paris (3ème chambre, 2ème section)* decision of 13 July 2007, available at: tinyurl.com/chv9lq
14) Indeed, this conclusion has been confirmed by a number of rulings, to the extent that the issue now seems settled in France; see, for example, Courtinat, A., *Persistence Pays Off for Comedian Bringing Cases against Video Share Sites*, available at: tinyurl.com/cc9gcf and Blocman, A., *Regional Court in Paris Confirms Host Status of Dailymotion*, available at: tinyurl.com/b5rdso
15) *Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique* (Act No. 2004-575 of 21 June 2004 on Confidence in the Digital Economy).
16) Jondet, N., *The Silver Lining in Dailymotion's Copyright Cloud*, available at: ssrn.com/abstract=1134807
17) SARL Zadig Productions, Jean-Robert Viallet et Mathieu Verboud v Sté Google Inc. et AFA, Tribunal de Grande Instance de Paris (3ème chambre, 2ème section), decision of 19 October 2007, available at: tinyurl.com/dbyyk6
18) Hardouin, R., *Observations sur les nouvelles obligations prétoriennes des hébergeurs*, available at: tinyurl.com/cdomwd
19) Jondet, N., *Google Video held liable for the copyright infringement of "Tranquility Bay" (TGI Paris 19 octobre 2007)*, available at: tinyurl.com/d79nvy
20) Cabrera Blázquez, F. J., *User-Generated Content Services and Copyright*, IRIS *plus* 2008-5, European Audiovisual Observatory.
21) Directive 2001/29/EC of the European Parliament and of the Council of

22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (InfoSoc Directive) [2001] OJ L167/10.

22) Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights, [2004] OJ L 157/45.

23) Van Eecke, P., Ooms, B., *ISP Liability and the E-Commerce Directive: A Growing Trend Toward Greater Responsibility for ISPs* 11(4) J. Internet L. 3.

24) *SABAM v SA Scarlet (anciennement Tiscali), Tribunal de Première Instance de Bruxelles*, 29 June 2007, available at: tinyurl.com/avnvj2

25) *SA Scarlet v SABAM, Tribunal de Première Instance de Bruxelles*, 22 October 2008.

26) *SA Scarlet Extended v SABAM, Tribunal de Première Instance de Bruxelles, No. 07/15472/A,* 22 October 2008.

27) Court of Bergamo, *Sezione penale del dibattimento in funzione di giudice del riesame*, *Ordinanza* of 24 September 2008, available at: tinyurl.com/48j2ow

28) Arena, A., *Italian Courts Ban Pirate Bay, but then Lift the Block*, IRIS 2008-10: 13, available at: merlin.obs.coe.int

29) *IFPI Danmark mod DMT2 A/S, Frederiksberg Byrets kendelse* of 29 January 2008.

30) Sandfeld Jacobsen, S., *Restraining Injunction against Internet Service Providers under Danish Law*, IRIS 2008-6: 7, available at: http://merlin.obs.coe.int/iris/2008/6/article10.en.html

31) Euractiv, *New EU Battle over Copyright Rules in Sight*, 30 January 2009, available at: tinyurl.com/d4kweh

32) Van Hoboken, J., *Freedom of Expression Implications for the Governance of Search*, in IRIS Special, *Searching for Audiovisual Content*, European Audiovisual Observatory, 2008.

33) Valgaeren, E., Roland, N., *YouTube and User-Generated Content Platform – New Kids on the Block?*, in IRIS *Special*, *Legal Aspects of Video on Demand*, European Audiovisual Observatory, 2007.

34) Commission report of 30 November 2007, SEC(2007) 1556, available at: tinyurl.com/awo7gr

35) European Parliament report on the outlook for copyright in the EU, INI/2008/2121, available at: tinyurl.com/cgqfuy

36) European Parliament resolution on cultural industries in Europe, INI/2007/2153, available at: tinyurl.com/djvoaj

37) Angelopoulos, C., *First Reading of New Telecoms Package*, IRIS 2008-10: 4 and *Council of the European Union: New Legislative Proposals for Telecoms Reform*, IRIS 2009-1: 5, available at: merlin.obs.coe.int

38) European Parliament legislative resolution of 24 September 2008, COM(2007)0698 – C6-0420/2007 – 2007/0248(COD), available at: tinyurl.com/6qwfxc

39) The rejected amendments of the Bono Report explicitly listed filtering as an example of co-operative ISP attitude.

40) European Parliament legislative resolution of 24 September 2008, COM(2007)0697 – C6-0427/2007 – 2007/0247(COD), available at: tinyurl.com/63t5pn

41) European Commission, *Commission proposes a single European Telecoms Market for 500 million consumers*, available at: tinyurl.com/d7nsb2

42) 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, 26 March 2008, available at: tinyurl.com/cna63u

43) Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (signed 4 June 1950, entered into force 3 September 1953).

44) Hugenholtz, P. B., *Copyright and Freedom of Expression in Europe*, in Dreyfuss, R. et al. (ed.), *Expanding the Boundaries of Intellectual Property. Innovation Policy for the Knowledge Society*, (Oxford University Press, New York 2001) 343-363.

45) See endnote 4 above.

46) Committee of Ministers of the Council of Europe, *Declaration on freedom of communication on the Internet*, 28 May 2003, available at: http://tinyurl.com/cpb6o6 . See also: Thórhallsson, P., *Declaration on Freedom of Communication on the Internet*, IRIS 2003-7: 3, available at: merlin.obs.coe.int

47) Barendt, E., *Freedom of Speech* (2nd ed., OUP, New York 2005) 247.

48) See Audible Magic Corporation response to the consultation, available at: tinyurl.com/3cw4mq

49) See endnote 4 above.

50) Informationsverein Lentia v. Austria, (App. No. 13914/88; 15041/89; 15717/89; 15779/89; 17207/90) ECHR 24 November 1993.

51) DailyMotion, *Dailymotion choisit la solution de fingerprinting d'Audible Magic pour détecter les vidéos protégées par des droits*, (13 July 2007) available at: http://www.dailymotion.com/press/AudibleMagic-Dailymotion.pdf

52) Stone, B., Helft, M., *New Weapon in Web War Over Piracy*, The New York Times, 19 February 2007, available at: tinyurl.com/38f527

53) BBC, *YouTube Rolls out Filtering Tools*, 16 October 2007, available at: tinyurl.com/byb42n

54) See endnote 16 above.

55) See endnote 9 above and Julià-Barceló, R., *On-Line Intermediary Liability Issues: Comparing E.U. and U.S. Legal Frameworks* 22(3) EIPR 105.

56) *Principles for User Generated Content Services*, available at: www.ugcprinciples.com

57) *The Principles for User Generated Content Services: A Middle-Ground Approach to Cyber-Governance*,121 HarvLRev 1387.

58) Ginsburg, J. C., *Separating the Sony Sheep from the Grokster Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs*, available at: tinyurl.com/dxwjtn

59) *Fair Use Principles for User Generated Video Content*, available at: tinyurl.com/demshm

60) *Accord pour le développement et la protection des œuvres et programmes culturels sur les nouveaux réseaux*, available at: tinyurl.com/2k73mn

61) Also known as the "three strikes (and you're out)" policy.

62) Courtinat, A., *Graduated Response according to the Bill on 'Creation and the Internet'* IRIS 2008-10: 10, available at: merlin.obs.coe.int

63) HM Treasury, *Gower's Review of Intellectual Property*, November 2006, available at: tinyurl.com/7xnsvn

64) *Joint Memorandum of Understanding on an Approach to Reduce Unlawful File-Sharing*, available at: tinyurl.com/abed4x.

65) Department for Business, Enterprise and Regulatory Reform (BERR), *Consultation on Legislative Options to Address Illicit Peer-to-Peer (P2P) File-Sharing*, July 2008, available at: tinyurl.com/5pxy6l

66) *Italy to Follow French Three Strikes Model for P2P*, 22 January 2009, available at: tinyurl.com/cusoca

67) *Downloaders face disconnection following Eircom settlement*, The Irish Times, 28 January 2009, available at: tinyurl.com/d45a3y

68) McBride, S., Smith, E., *Music Industry to Abandon Mass Suits*, The Wall Street Journal, available at: tinyurl.com/4h9omj

69) See Microsoft, Google, EuroISPA and UK responses to the consultation, available at: tinyurl.com/3cw4mq