

CROWELL & MORING LLP WHITE PAPER: ISP LIABILITY FOR ONLINE INFRINGEMENT IN EUROPE

In Europe, as in the United States, Internet Access Providers have conditional immunity under the law against liability for infringing activity by their users. In balancing the interests of copyright owners in protecting their intellectual property from piracy with the interests of ISPs in serving their non-infringing users, European courts and legislative bodies have developed a set of rights and remedies to address the issue as it continues to develop. The following is a summary of the legal framework and a number of recent cases regarding intermediary liability in Europe.

1. European Legal Framework

Article 12.1° of Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (the “E-Commerce Directive”) provides that internet access providers cannot be held liable for the information transmitted on their networks:

*“Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider **is not liable for the information transmitted**, on condition that the provider:*

- (a) does not initiate the transmission;*
- (b) does not select the receiver of the transmission; and*
- (c) does not select or modify the information contained in the transmission.”*

Article 15.1° of the E-Commerce Directive moreover specifies that internet access providers should not be made subject to general obligations to monitor the information transmitted on their network:

*“Member States shall **not impose a general obligation** on information providers, when providing the services covered by Articles 12, 13 and 14, **to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.**“*

However, this immunity for internet access providers does not mean that they cannot be required to contribute to the fight against infringing activity on the internet. The preamble to Directive

2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society (the “Directive 2001/29”) reads as follows:

*“In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. **In many cases such intermediaries are best placed to bring such infringing activities to an end.** Therefore, without prejudice to any other sanctions and remedies available, **rightholders should have the possibility of applying for an injunction against an intermediary who carries a third party’s infringement of a protected work or other subject-matter in a network.**”*

Article 8.3° of Directive 2001/29 provides the following:

“Sanctions and remedies

*3. Member States shall ensure **that rightholders 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.”*

Directive 2004/48/EC on the enforcement of intellectual property rights (hereafter the “Enforcement Directive”) contains a similar provision. Article 11 of the Enforcement Directive provides that:

*“(…) Member States shall also ensure **that rightholders are in a position to apply for an injunction against intermediaries** whose services are used by a third party to infringe an intellectual property right, without prejudice to Article 8(3) of Directive 2001/29/EC.”*

Both Directive 2001/29 and the Enforcement Directive confirm that measures taken in this context shall be equitable and proportionate¹ and strike a fair balance between the interests of the copyright owners and those of the internet access providers and internet users. In the words of the European Court of Justice: *“national authorities and courts must, in particular, strike a fair balance between the protection of the intellectual property right enjoyed by copyright holders and that of the freedom to conduct a business enjoyed by operators such as ISPs pursuant to Article 16 of the Charter”*.

Accordingly, in the EU, internet access providers do not have a duty to actively seek infringing activity committed over their networks.² However, notwithstanding the immunity from liability they enjoy under the E-Commerce Directive, they can be required by courts to take

¹ Article 3 of the Enforcement Directive.

² Article 15 of the E-Commerce Directive.

measures aimed not only at bringing to an end infringements already committed against intellectual property rights using their services, but also at preventing further infringements.³ The European Court of Justice nevertheless has repeatedly insisted that such measures should not equate to a general monitoring obligation, and that they should not be disproportionate.⁴

2. Application In Practice: DNS Blocking

National Courts of several member states of the European Union have imposed injunctions requiring internet access providers to implement DNS blocking measures with respect to websites containing illegal content:

- In Denmark, the Danish Supreme Court upheld an order granted on application of the Danish branch of IFPI requiring internet access provider Telenor to block access to www.thepiratebay.org (“the Pirate Bay”) by means of DNS blocking;⁵
- In Austria, the Commercial Court of Vienna ordered UPC Telekabel Wien to implement IP blocking in respect of the website www.kino.to, which offers copyright infringing movie on demand services to German and Austrian viewers;⁶
- In Belgium, the Court of Appeal of Antwerp required two internet access providers to implement DNS blocking with respect to several domains of The Pirate Bay.⁷ In its order, the Court confirmed that:
 - The internet access providers do not need to monitor the internet but must only block access to the domains specifically listed in the judgment;
 - The internet access providers must only implement a specifically identified technical measure, i.e. DNS blocking, and cannot be held liable in case of circumvention by subscribers or The Pirate Bay;
 - DNS blocking is a proportionate measure since it is technically easy to implement and does not trigger important costs or investments;

³ Article 8,3° of Directive 2001/29 and 11 of the Enforcement Directive. Case C-324/09, *L'Oréal v Ebay* [2011] ECR I-0000, paragraph 131.

⁴ See Case C-324-09, *L'Oréal v Ebay* [2011], paragraph 139 and Case C-70/10, *Scarlet v Sabam* [2011], paragraph 36.

⁵ *Telenor v IFPI* (Danish Supreme Court, 27 May 2010).

⁶ *Constantin Film v UPC Telekabel Wien* (Handelsgericht Wien, 17 May 2011).

⁷ *Baf v Telenet* (Court of Appeal Antwerp, 26 September 2011).

These different injunctions are currently still in force and operational without raising significant issues. There is, however, a fair amount of circumvention both by subscribers using different DNS servers and by the infringing websites moving to different domains.

3. **Scarlet v. Sabam: Monitoring and Filtering**

By judgment of 29 June 2007, the President of the Court of First Instance of Brussels ordered internet access provider Scarlet, on pain of a periodic penalty, to bring copyright infringements to an end by making it impossible for its customers to send or receive files containing a musical work in the repertoire of copyright collecting society Sabam by means of peer-to-peer software. This Court order effectively required Scarlet to filter all peer-to-peer traffic over its network in order to block exchanges of copyright infringing material.

Scarlet lodged an appeal against this judgment with the Court of Appeal of Brussels, which took the view that, before determining whether a mechanism for filtering and blocking peer-to-peer files was actually available and could be effective, the Court had to be satisfied that the obligations liable to be imposed on Scarlet were in accordance with European Union law. It therefore referred the case to the European Court of Justice.

On 24 November 2011, the European Court of Justice held that “*the injunction imposed on the ISP concerned requiring it to install the contested filtering system would oblige it to actively monitor all the data relating to each of its customers in order to prevent any future infringement of intellectual-property rights. It follows that that injunction would require the ISP to carry out general monitoring,*” which would be contrary to article 15 of the E-Commerce Directive.

The Court in addition considered that “*such an injunction would result in a serious infringement of the freedom of the ISP concerned to conduct its business since it would require that ISP to install a complicated, costly, permanent computer system at its own expense*”, which would be contrary to the condition that measures to ensure the respect of intellectual property rights should not be unnecessarily complicated or costly. The Court therefore held that “*the injunction to install the contested filtering system is to be regarded as not respecting the requirement that a fair balance be struck between, on the one hand, the protection of the intellectual-property right enjoyed by copyright holders, and, on the other hand, that of the freedom to conduct business enjoyed by operators such as ISPs.*”

The Court furthermore considered that “*the injunction requiring installation of the contested filtering system would involve a systematic analysis of all content and the collection and identification of users’ IP addresses from which unlawful content on the network is sent. Those addresses are protected personal data because they allow those users to be precisely identified.*” and that it “*could potentially undermine freedom of information since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications. Indeed, it is not contested that the reply to the question whether a transmission is lawful also depends on the application of statutory exceptions to copyright which vary from one Member State to another. Moreover, in some Member States certain works fall within the public domain or can be posted online free of charge by the authors concerned.*”

Consequently, the Court held that, in adopting the injunction requiring the ISP to install a filtering system, the national court would not be respecting the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the right to protection of personal data and the freedom to receive or impart information, on the other.⁸

4. European cases imposing sanctions notwithstanding various levels of non-infringing use

In *20th Century Fox v BT* the English High Court decided that BT could be ordered to block access to the domains of Newzbin2 and that such order is proportionate and does not affect fundamental rights of BT and users of the internet.⁹ The Court considered in this context that “*The position might be different if Newzbin2 had a substantial proportion of non-infringing content, but that is not the case.*” The factual evidence in that case showed that more than 95% of all content offered via Newzbin2 was copyright infringing.

In *Baf v Telenet*, the Court of Appeal of Antwerp found that the fact that not all content made available through The Pirate Bay was copyright infringing did not suffice to reject the application for an injunction. It stated that “*a very substantial proportion of the content was infringing*” and that the non-infringing content would surely be available elsewhere. At the same time, the Court rejected an approach based on IP blocking, for fear of undesired effects on the legitimate activities of third parties (e.g., that a legitimate website hosted on the same servers as an illegal website would be blocked as result of IP blocking).

⁸ Case C-70/10, *Scarlet v Sabam* [2011].

⁹ [2011] EWHC 1981 (Ch).

Finally, in *Scarlet v Sabam*, the European Court of Justice considered that the injunction applied for could potentially undermine the fundamental freedom of information, since the filtering system contemplated “*might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications.*”¹⁰ The Court invoked this risk of blocking lawful content as part of the reasons for considering that the filtering system contemplated was disproportionate. Similar considerations might apply in the context of DNS blocking of websites containing a mix of lawful and unlawful content. Hence, following the European Court of Justice’s recent ruling in *Scarlet v Sabam*, it is as yet not clear how much impact on legitimate activities will be deemed acceptable in the context of balancing the interests of owners of intellectual property rights and the rights of users of the internet.

Thomas De Meese
Crowell & Moring LLP
Rue Joseph Stevens 7
B - 1000 Brussels
Belgium
Tel: + 32 2 282 40 82
tdemeese@crowell.com

John I. Stewart, Jr.
Crowell & Moring LLP
1001 Pennsylvania Avenue NW
Washington, DC 20004
Tel: 202 624-2685
jstewart@crowell.com

¹⁰ Case C-70/10, *Scarlet v Sabam* [2011], paragraph 52.