INTERNET COPYRIGHT INFRINGEMENT: REMEDIES AGAINST INTERMEDIARIES — THE EUROPEAN PERSPECTIVE ON HOST AND ACCESS PROVIDERS

by Jan Bernd Nordemann*

I. INTRODUCTION

Copyright is everywhere. And so are copyright infringements, particularly on the Internet. The reasons why copyright infringements can be found so extensively on the Internet are similar in many countries worldwide and are of a complex nature. A key reason, however, relates to the nature of the Internet itself. Generally speaking, infringers are able to commit their infringing acts anonymously, and investigating the identity of the person or persons responsible is a costly, time-consuming process and is often impossible. The disadvantage of bringing an action against individual infringers is that each infringement has to be prosecuted individually — a process that is laborious and expensive considering the sheer number of infringements involved. Therefore, it is logical to consider not only taking action against the infringing consumers, but also against the Internet intermediaries used by the consumers, in particular, suppliers of Internet services that provide infringers with the relevant infrastructure and thus make the copyright violations possible in the first place. Legal action against such providers may even have a much greater effect than that against individual perpetrators, as for example the German Federal Court of Justice (Bundesgerichtshof, BGH) has already recognized.¹

This article therefore looks at hosting providers and access providers (mere conduits) as the main intermediaries on the Internet with respect to possible remedies against them under European law in case their services are used for copyright infringement. Also, it will be investigated to what extent EU law allows the identification of infringing consumers through their (dynamic) IP-address and using information claims against Internet access providers. But one has to start with some general remarks on the


* German attorney-at-law, certified copyright and media attorney and certified intellectual property attorney, Anwaltssozietaet Boehmert & Boehmert, Berlin; honorary professor at the Humboldt-University in Berlin; j.nordemann@boehmert.de. The author greatly appreciates the input of Corey Field, Ballard Spahr LLP, Los Angeles, on aspects of U.S. copyright law.
EU framework with respect to copyright infringements and Internet intermediaries.

II. EU LAW FRAMEWORK

U.S. copyright law is federal law, directly applicable in all U.S. states. For copyright law, this is different in the EU. There is no community-wide copyright law. Rather, European copyright law consists of a bundle of national copyrights. This national copyright is regulated by separate national copyright laws in each EU Member State. This is confirmed by Article 8, paragraph 1, of the EU Rome II Regulation.\(^2\) In international conflict of laws, the country-of-protection principle governs the laws of the EU-Member States: “The law applicable to a non-contractual obligation arising from an infringement of an intellectual property right shall be the law of the country for which protection is claimed.” European legislators, however, tried to harmonize certain aspects of the national copyright laws throughout the EU through several directives, which had to be “implemented” by each national legislature. Some of these EU directives also set a certain framework for remedies against Internet providers just as the U.S. DMCA does. The Court of Justice of the European Union (“CJEU”) in Luxemburg rules on national copyright cases as far as they involve unclear questions of national copyright law, which were harmonized by such EU directives.

A. Liability Privileges

EU law makes it mandatory for Member States to grant liability privileges for Internet providers. Articles 12 to 14 of the EU E-Commerce Directive\(^3\) stipulate that Member States’ legislatures must establish liability shields for access providers (mere conduits), caching providers and hosting providers. These liability shields also cover claims for copyright infringement, yet only cover particular damages and criminal liability. Unlike the U.S. DMCA, they do not cover injunction claims.

B. Injunction Claims

In particular, the liability privileges do not apply to claims for injunctive relief pursuant to Article 11, third sentence, of the Directive 2004/48/EC (so-called “Enforcement Directive”) and Article 8, paragraph 3, of the


Internet Copyright Infringement

Directive on the harmonization of certain aspects of copyright and related rights in the information society⁴ “EU Copyright Directive.” Article 8, paragraph 3, of the EU Copyright Directive requires the national legislature to provide for claims against “intermediaries” whose services are used for copyright infringements.

There is no problem with classifying access, caching and hosting providers as “intermediaries” in the sense of the two directives.⁵ Recital 23 of the Enforcement Directive and Recital 59 of the EU Copyright Directive leave “conditions and procedures” for such injunction claims to the Member States. These Recitals, however, do not grant carte blanche to Member States to set any requirements they wish. Rather, the liability requirements in national tort and contributory liability law limited by Articles 12 to 14 of the EU E-Commerce Directive have to be subordinate to claims under Article 11, third sentence, of the Enforcement Directive and Article 8, paragraph 3, of the EU Copyright Directive. Otherwise the separate provisions of Article 11, third sentence, of the Enforcement Directive and Article 8, paragraph 3, of the EU Copyright Directive would be superfluous.

Recital 59 of the Enforcement Directive also expressly states that the claims against the “intermediary” pursuant to Article 8, paragraph 3, of the EU Copyright Directive must exist even if the “acts carried out by the intermediary are exempt under Article 5 [of the EU Copyright Directive].” In the report of the European Commission analysing the application of the Enforcement Directive, the European Commission highlighted that neither Article 11, third sentence, of the Enforcement Directive nor Article 8, paragraph 3, of the EU Copyright Directive had any require-ment of liability.⁶ In its L’Oréal v. eBay decision, the CJEU confirmed this approach. In this decision, the CJEU held that Article 11, third sen-

ence, of the Enforcement Directive could be applied “regardless of any liability” of the provider.\footnote{7}

The concept behind this is further explained in Recital 59 of the EU Copyright Directive. The Directive first states that “in the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities.” But it goes on to emphasize: “In many cases such intermediaries are best placed to bring such infringing activities to an end.” In other words: The reason, why injunction claims may be raised under Article 8, paragraph 3, of the EU Copyright Directive, is not based on the contribution of the providers; they have not done any legal wrong.\footnote{8} But it is the fact that they are in a good position to help.\footnote{9} This is comparable — to a certain extent — to helping duties existing in the general civil law of the Member States, e.g., known in English law as the \textit{Norwich Pharmacal} jurisdiction\footnote{10} or the German concept of helping duties in case of accidents. This seems to be in contrast to the underlying concept of U.S. law, which even under the DMCA remains a contribution-based legal system in case injunction claims are raised against Internet service providers.

If the EU concept for injunction claims relies on helping duties, the question arises to what extent the helping intermediaries can ask for cost reimbursement. Certain national systems in the EU — such as the German or the English system — would allow cost reimbursement in case of injunction claims due to helping duties. But the EU law concept for intermediaries in Article 8, paragraph 3, of the EU Copyright Directive and Article 11, third sentence, of the Enforcement Directive is different and requires the intermediaries to pay the costs to fulfil their help duties. Therefore, even if under national concepts cost reimbursement could be asked for by the party obligated to help, the providers as intermediaries have to pay the costs of fulfilling their help duties, which arise from the EU Copyright Directive.\footnote{11} The CJEU seems to have confirmed this. In

\footnotesize{
\textsc{SEC(2010) 1589 final, at 16-17 (Dec. 22, 2010); for the same opinion, see Shapiro, supra note 5, at 54.}
\footnote{7} \textsc{Case C-324/09 ¶ 127, L’Oréal v. eBay (2011), [2012] E.M.L.R 6.}
\footnote{8} \textsc{Twentieth Century Fox Film Corp. v. British Telecommunications, PLC, [2011] EWHC 2714 (Ch.).}
\footnote{9} \textsc{Shapiro, supra note 5, at 55.}
\footnote{10} \textsc{Norwich Pharmacal Co. v. Customs & Excise Comm’rs, [1974] AC 133 (explained in detail, \textit{Twentieth Century Fox} ¶¶ 20 et seq. [2011] EWHC 2714(Ch)).}
\footnote{11} \textsc{Twentieth Century Fox, [2011] EWHC 2714 ¶ 30; see also with respect to German law, Jan Bernd Nordemann, \textit{Haftung von Providern im Urheberrecht – Der aktuelle Stand nach dem EuGH-Urteil v. 12. 7. 2011 – Eugh 12.07.2011 Aktenzeichen C-324/09 – L’Oréal/eBay GRUR 977, 979 (2011).}
Internet Copyright Infringement

*L’Oréal v. eBay*, the CJEU held that measures by the providers must not be “excessively costly.”

**C. Conflict of Laws**

Pursuant to Article 8, paragraph 1, of the EU Rome II Regulation, the law applicable to infringements of copyright shall be the law of the country for which protection is claimed. This is also referred to as the territoriality principle. With respect to infringements via the Internet, it is sometimes difficult to assess if an infringement was committed in the territory of the Member State. This is particularly true for all acts of public communication and foremost for the publicly making available right (Article 3, paragraph 1, of the EU Copyright Directive). In the case of publicly making available on the Internet, it is disputed whether the making available takes place both at the server location (EU Member State A) and at the place where the content made available is received via the Internet and displayed (EU Member State B). In a database right case, the CJEU made clear that “at least” where there is an intention on the part of the person performing the act to target members of the public in Member State B, the database right is used in EU Member State B. But the mere accessibility of the trader’s or the intermediary’s Web site in the Member State in which the consumer is domiciled is insufficient.

The Luxemburg Court gave some hints as to elements that could speak in favour of a Web site targeting another EU-Member State: content interesting for the public in the target country (e.g., England as the target country, if content is about betting on matches of the Football English Premier League); mention of itineraries from other Member States for going to the place where the trader is established; use of a language or a currency other than the language or currency generally used in the Member State in which the trader is established, with the possibility of making and confirming the reservation in that other language; mention of telephone numbers with an international code; outlay of expenditure on an Internet-referencing service in order to facilitate access to the trader’s site or that of its intermediary by consumers domiciled in other Member States; use of a top-level domain name other than that of the Member State in which the trader is established; and mention of an international clientele composed of customers domiciled in various Member States.

12 Case C-324/09 ¶ 39, *L’Oréal*.


14 *Id.* ¶ 36.

15 Case C-324/09, ¶ 40-42, *L’Oréal; see also* Joined Cases C-585/08, C-144/09 ¶¶ 75-93, Pammer v. Karl Schlüter, GmbH KG; Hotel Alpenhof v. Heller ¶¶ 75-93 (CJEU 2010).
It is for the national courts to ascertain whether sufficient evidence exists to show that a Web site is targeted (also) at the other EU-Member State. In *L’Oréal v. eBay*, the Court held that the rules of Trade Mark Directive 89/104 and Trade Mark Regulation 40/94 apply as soon as it is clear that the offer for sale of a trade-marked product located in a third State is targeted at consumers in the territory covered by the trade mark.\(^\text{16}\) Thus, an EU Member State is the country of protection and may apply its national copyright law if the infringing copyrighted content is intended to be downloaded or streamed by users in this EU Member State. This also is in line with national case law, e.g. of Germany, where the German Federal Court of Justice (*Bundesgerichtshof*, BGH) applied German copyright law to all acts of making available on the Internet pursuant to Article 3, paragraph 1, of the EU Copyright Directive, to the extent that they are (also) intended to reach German users.\(^\text{17}\) All infringements in the language of the protecting country should meet this requirement. For the French-speaking part of Belgium, this should be true even if the Web site used a French domain name, in particular if there is no registration requirement or if registration is also open to users not domiciled in France. As to offers in other languages, a movie made available could also be intended for users in the protecting country, if the foreign language is the original language of the movie and it has not yet been released in the protecting country; in this case it is also of interest to users in the protecting country. This is particularly true if the foreign language is widely spoken, e.g. English. Also, advertisements on the Web site addressed to users in the protecting country can be a factor to show the relevant intent. Therefore, it can be expected that European law allows the protecting country a considerable influence on the behaviour of providers even if located outside the protecting country.

### III. REMEDIES AGAINST HOSTING PROVIDERS

#### A. Types of Hosting Providers

Up to now, numerous business models for host providers have been developed which in part overlap. Several business models will be outlined below.

\(^{16}\) Case C-324/09 ¶¶ 61-52, *L’Oréal*.

\(^{17}\) See Bundesgerichtshof [BGH] [Federal Court of Justice], Wagenfeld-Leuchte, file no. I ZR 114/04 (Feb. 15, 2007), GRUR 2007, 871, 872 (2007); see also Jan Bernd Nordemann, in Friedrich Fromm & Wilhelm Nordemann, *Urheberrecht: Kommentar zum Urheberrechtsgesetz, Verlagsgesetz, Urheberrechtswahrnehmungsgesetz* [Commentary: German Copyright Act] (10th ed. 2008) (discussing section 105 UrhG, n.10; Nordemann-Schiffl, in *id* before section 120 nn. 96 et seq.
“User Generated Content” sites (also known as “UGC” sites): these enable users to store their own content on a platform. In order for such content to be found by the public, the hosting provider usually provides a particular structure for the storage or at least the possibility of searching. Examples of such “user generated content” sites are Internet auction platforms (e.g., eBay), platforms for storage and making available of video files (e.g., YouTube), of photographs (e.g., Flickr), of links (e.g., alluc.org, g-stream.in), and of discussion boards or content of social networks (e.g., Facebook). The susceptibility to infringements can be seen from the offer of particular categories such as “current feature films,” “series” (e.g., www.g-stream.in) or “Audio Books.”

File hosts: some hosting providers limit themselves to the mere provision of storage space. This is partly realized in return for payment for the storage of any content (e.g., the large German host provider 1&1), while others allow the storage of any content free of charge, but fund themselves through other features such as payment for an increased download speed (e.g., cyberlockers such as Rapidshare). The key feature of these types of business is that the hosting provider does not offer the customer any structure for the content they store, in particular no categorization thereof.

Link sharing sites: numerous Web sites have emerged on the Internet that make available links to files stored with file hosts. Such sites are known as link-sharers (also “linking sites”) and they offer a categorization and searching possibilities (e.g., alluc.org, kino.to). These are often UGC sites, i.e., the links are posted by the users. Link sharing sites are usually especially susceptible to infringement. For example, link sharers such as kino.to usually contain links to copies of many current cinema films that are stored with file hosts.

Link referrers: other hosting providers have business models between the previous two mentioned. So-called link referrers encrypt the collections of links (to files stored with file hosts) made available by link-sharers, sometimes preparing access to such files in a download-friendly manner. This makes it more difficult for the rights holder to determine the storage location at the file host and in turn to identify the source at the file host. Hence, an increased encryption of such rights-infringing links may frustrate enforcement.

Index hosts: host providers also exist who make their servers available for an index to be made available via the internet.
This is designed to make it easier for the user to find particular content. Such indices are often compiled automatically by a software program. The most well-known index is produced by Google with the hits generated by its search engine; in this case, the index refers to the entire internet. Indices can, however, also refer to smaller networks within the internet. The Piratebay.org is a search engine for locating film and music files within the BitTorrent network, the vast majority of which are illegal.

B. Liability Privilege for Host Providers (Article 14 of the EU E-Commerce Directive)

Hosting providers are in the “safe harbor” pursuant to Article 14 of the EU E-Commerce Directive if the hosting provider is (1) an intermediary that stores users’ content, and (2) has no actual knowledge of illegal activity. Additionally, to enjoy the safe harbor with respect to damage claims, the hosting provider (3) must not be aware of facts or circumstances from which illegality is apparent.

For U.S. lawyers, these requirements look familiar, as they can be found in a somewhat different wording in the U.S. DMCA. Section 512(c)(i)(a) mentions requirements such as no actual knowledge and not being aware of facts from which infringing activity is apparent.

In L’Oréal v. eBay, the CJEU interpreted the aforementioned requirements in Article 14 of the EU E-Commerce Directive to apply to the liability privilege. To qualify as an intermediary storing users’ content, the hosting provider must not play an active role in order to give the provider knowledge or control over its user’s content. The provider must take a “neutral” position as to user’s content. The provider plays an active role if it optimizes the presentation of the user’s content or promotes it. However, national EU courts struggle with these requirements for the “liability privilege” of Article 14 of the EU E-Commerce Directive. One example in the copyright world is YouTube. The Spanish Mercantile Court Madrid and the District Court (Landgericht) Hamburg regarded You-

20 Case C-324/09 ¶ 113, L’Oréal.
21 Id. ¶ 116.
22 Id.
Internet Copyright Infringement

Tube as an intermediary hosting third-party content, while earlier a different division of the District Court Hamburg saw YouTube as a direct infringer, making the UGC content its own content.

The CJEU in *L’Oréal v. eBay* also explored the requirements that the hosting provider must not have actual knowledge of illegal activity and — in particular to defend damage claims — must not be aware of facts or circumstances from which illegality is apparent. The CJEU held that the “diligent economic operator” is the standard. One has to ask the question of whether the hosting provider “should have identified the illegality in question.” Awareness may be created by the right-holder through a notice-and-takedown-letter (NTD-letter). Under EU law, the content of such a NTD-letter is not specifically addressed as in the U.S. DMCA. Rather the content follows from its function in EU law to create actual knowledge and make the provider act as a “diligent economic operator.” To illustrate this: YouTube as a hosting provider will lose its liability privilege for damage claims under Article 14 EU of the E-Commerce Directive if it is made aware of an identical copy of a recent theatrical movie uploaded onto its servers. But the situation may get more complex if users adapt the original work. One example could be a mash-up between a movie and an uploader’s own dubbing. Under certain circumstances, this could qualify as a legal caricature or parody (Article 5, paragraph 3(k) of the EU Copyright Directive). It seems to be an open question in such scenarios to what extent a “diligent economic operator” is able to identify illegality.

C. Injunction Claims Against Hosting Providers

As shown above (II 2.), in contrast to the U.S. DMCA, the liability privilege of Article 14 of the EU E-Commerce Directive does not apply to claims for injunctive relief pursuant to Article 8, paragraph 3, of the EU Copyright Directive. Article 8, paragraph 3, of the EU Copyright Directive requires the national legislature to provide for claims against “intermediaries” whose services are used for copyright infringements. In its *L’Oréal v. eBay* and *Netlog* decisions, the CJEU had the opportunity to clarify what mandatory framework is set for the Member States by Article 8, paragraph 3, of the EU Copyright Directive (and its sister provision Article 11, third sentence, of the Enforcement Directive for other IP rights). To understand this case law better, a look into the Member States’ case law seems to be valuable.

---

According to the longstanding case law in Germany — in particular in the so-called Internet auction cases of the Bundesgerichtshof (BGH) — upon becoming aware of a clear rights infringement, duties of care arise for the hosting provider under the famous “Stoererhaftung” [literal translation: “disturber’s responsibility”] doctrine not only to delete a rights infringement, but also to prevent further rights infringements, for which there are specific grounds, through checking content. Duties of care can then exist in three respects:

- The provider must takedown the specific clear infringement from the Internet;
- A further duty of care exists to prevent the repetition of the specific clear infringement as described in the NTD-letter. German courts justify this duty through the risk of repetition of the specific clear infringement, if it already occurred once;
- Furthermore in case of clear infringements, a duty of care has been recognized to prevent other infringements of the same type and just as clearly recognizable. In this respect, the breach of duty of care exceeds the direct infringer’s and the contributing infringer’s liabilities, which only apply to the specific infringement due to the requirement of intent. This was justified by the Court based on the existing risk of first infringements of the same type and just as clearly recognizable.

Internet Copyright Infringement

including host providers. The High Court of Justice Chancery Division (England and Wales) in L’Oréal v. eBay referred to the Court of the European Union (CJEU) as question number 10, while commenting that the case law of the Bundesgerichtshof (BGH) “is entitled to the greatest of respect.” The Advocate General in his opinion in particular referred to Article 3, paragraph 2, of the Enforcement Directive and its principle (“Those measures, procedures and remedies shall also be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse”). He came to the conclusion that EU law does not prohibit further duties for host providers than to filter the specific infringement, but there was no obligation of Member States to provide such claims, as “the conditions and procedures relating to such injunctions are defined in national law.”

In its L’Oréal v. eBay decision, the CJEU confirmed the German case law. According to the court, Article 11, sentence 3, of the Enforcement Directive even required the Member States “to ensure . . . to order the operator of an online market place to take measures which contribute, not only to bringing to an end infringements of these rights by users of the market place, but also to preventing further infringement of that kind.” This goes further than the Advocate General’s opinion, which had left such duties of prevention to the Member States. But the Luxemburg Court further expressed that the rules for the operation of the injunctions under Article 8, paragraph 3, of the EU Copyright Directive, such as those relating to the conditions to be met and to the procedure to be followed, are a matter for national law.

At any rate, German case law seems convincing. A general duty of care in the sense of Article 15 of the EU E-Commerce Directive is not established. Rather, such a duty of care to look for clear infringements of the same type, which are just as clearly recognizable, is limited to scenarios that are likely to occur. For less likely scenarios, the duty of care does not apply. Also, the host provider in principle seems to be best placed to stop

---

30 See [2009] EWHC 1094, ¶ 326 (Ch.) (decision of 22 May 2009).
31 Case C-324/09, ¶¶ 127, 128-34, L’Oréal.
32 See Nordemann, supra note 11, at 980.
33 C-324/09, ¶ 135, L’Oréal.
such future (likely) infringements from happening, as it is its own customers within its own infrastructure that will commit the infringements.

Recent U.S. case law does not seem to be on this path. For example, according to the Ninth Circuit in *UMG v. Veoh*, the copyright owner must send a notice, e.g., with a specific URL address for the infringing file. Using “digital watermarking” to take down all the same files is not required under the DMCA. This can be one of the most frustrating aspects of U.S. law for copyright owners: they may send a “notice” and have a specific file taken down, but the same file keeps being posted over and over by other users. The ISP has no obligation to “look for” other infringements of that kind, only an obligation to respond to a “notice” that gives a specific file location.

With respect to the filtering duties for merely similar infringements under EU law, there is, however, an “outer limit” set by a later CJEU decision in *Netlog*. The CJEU held that requiring duties of a host provider to filter its entire content stored for copyright breaches would not be in line with Article 15 of the EU E-Commerce Directive: A filtering system to prevent copyright breaches for copyrighted files, which (1) applies indiscriminately to all users (2) as a preventive measure and (3) exclusively at the expense of the host provider and (4) for an unlimited period may not be demanded from host providers under Article 8, paragraph 3, of the EU Copyright Directive. But the European approach has not yet answered all questions. In particular, some open questions remain in respect to the following four issues:

1. **Duty of Care to Prevent a Specific Infringement**

Under EU law, all hosting providers — regardless of business model — are subject to the obligation of in the future preventing a “clear” (point 3 below) specific rights infringement of which they have become aware. This runs parallel with recent U.S. case law.

In this context, the host provider must in any case delete the specific infringements of which he has been made aware, and prevent such content being stored in his data storage space again. No cases are known in which the hosting provider was unable to permanently block the specific rights infringing content. In order to filter rights-infringing files, so-called hash filters can be used with the help of which a file can be identified as identical. In the case of file hosts such as Rapidshare, these hash filters are known as “MD5 filters.” Other infringements, such as illegal links on link-
referrer sites, on streaming sites such as YouTube or in search engine results, can also be reliably blocked through respective keyword filters. A particular feature applies to the “original” Usenet provider: following a “cancel request” by the rights holder, the Usenet provider is then responsible for deleting the rights-infringing file throughout the entire Usenet (via Usenet rules, which apply between the providers; a so-called kill command).36

It seems, however, as yet unclear under EU law, whether the duty of care for the hosting provider also exists if the provider is made aware of an “unclear” (point 3) rights infringement. Fundamentally, any requirements of the unlawfulness which limit the duty of care to take down and prevent the re-upload of the specific infringement should not be relevant. Mere unlawfulness should be enough to trigger such a duty of care. It is down to the risk of the hosting provider as to whether he decides to enter into the dispute between his customer and the rights holder. The hosting provider has chosen its (file storing) customers.

2. Duty of Care to Prevent “Other Infringements of That Kind”

In contrast to recent U.S. case law, however, the prevention duties of a hosting provider go further than taking down the specific infringement and preventing it from being re-uploaded. Following the German Bundesgerichtshof, the CJEU established duties for the hosting provider to prevent “further infringements of that kind” (see above). It is an unanswered question which copyright scenarios can be defined as being of “that kind.” This article proposes the following assessment under copyright law.37

- Infringements are of the same kind if the same work is affected and the same copy (in another file) or another clearly infringing copy has been used.38 For example, the same type exists under copyright law if a video portal stores and makes available the same cinema film in another file as that in the notice and takedown letter. An infringement of the “same kind” also would be found if a link referrer made another link to the same film available to the public.
- But one can ascertain that duties of care to block the same kind of infringements which are also clearly recognisable do not only refer to the same work. Rather, an obligation to block can also exist for other

---

37 For details regarding the German law background, see Nordemann, supra note 27, ¶ 130 et seq.
works. The repeat offender argument is particularly relevant here; but even if the service otherwise demonstrates an increased susceptibility to infringement, a duty of care could exist for other works.39

3. “Clear” Infringement?

As we have seen, the case law of the German Bundesgerichtshof only recognized prevention duties after clear infringements of IP rights with respect to other infringements of the same type and just as clearly recognizable.40 The CJEU in L’Oréal v. eBay only spoke of a duty to prevent “further infringement of that kind,” without setting the pre-condition of a clear infringement to have occurred.41 But in any case, the CJEU requested that only measures may be asked from the providers, which are “effective and dissuasive,” “fair and proportionate and . . . not . . . excessively costly,” and “effective and proportionate.”42 Therefore, also in case law of the CJEU, the “clarity” of the infringement can be of relevance, as the prevention duties will rise with the clarity of the infringement.

Defining a “clear” infringement under copyright law requires objective criteria. While one can expect a hosting provider to employ staff trained in copyright law, according to the German Bundesgerichtshof one cannot expect that the host provider employs well-trained lawyers.43 The making available to the public of identical copies of copyright protected works — whether they are film works, music works, audio books or photography — would accordingly be a “clear” infringement; they form the vast majority of infringing works made available on the Internet. The use of original or unamended works is also a “clear” infringement, provided that exceptions and limitations to copyright protection (Article 5 of the EU Copyright Directive) cannot seriously be applicable. Examples of infringements which are not “clear” would be, e.g., borderline cases of parody, satire and pastiche.

The obviousness of the infringement plays a decisive role, but so too should the “clarity” of the right to take action (“chain of title”). However, this cannot mean that works with a complicated chain of title can no longer be “clearly” infringed; this would discriminate against older works,

39 See Nordemann, supra note 28, ¶ 30 et seq.
40 Concerning trademark law, see Bundesgerichtshof [BGH] [Federal Court of Justice], Internetversteigerung III, file no. I ZR 73/05, Apr. 30, 2008, GRUR 702, 706 n.51 (2008); Bundesgerichtshof [BGH], Internetversteigerung II, file no. I ZR 35/04, GRUR 708, 712 n.45 (2007). For a discussion about the duty of care under German law, see Nordemann, supra note 27, ¶ 35 et seq.
42 Id. ¶¶ 136, 139, 141.
43 See Bundesgerichtshof [BGH] [Federal Court of Justice], Kinderhochstuehle im Internet, file no. I ZR 139/08, July 22, 2010, GRUR 152 n.48 (2011).
e.g., older films that have changed title several times. It cannot be the case that works with a complicated chain of title do not trigger a duty of care and their rights holders are therefore unable to effectively take action against copyright infringements on the Internet. The right to take action is “clear” if no justified doubts of the hosting provider as to such a right exist. The rights holder can disclose the chain of title by way of substantiation. That is not necessary, however. Justified doubts of the hosting provider are already considered not to exist if the hosting provider can trust the information in the NTD letter stating rights ownership. Any declarations which expose the right-holder to the risk of criminal prosecution in the event of provision of false information should suffice. The rights holder can also guarantee to hold the hosting provider harmless in case the latter acts on the former’s instructions. In addition, the rights holder can cite the legal assumptions derived from Article 5 of the Enforcement Directive.


In *L’Oréal v. eBay*, the CJEU held that only measures may be asked from the providers that are “effective and dissuasive,” “fair and proportionate and . . . not . . . excessively costly,” and “effective and proportionate.” As a result, such language seems to come down to a proportionality test for the measures of the hosting provider. Whether or not a measure of the hosting provider is proportionate has to be decided on a case-by-case basis after a comprehensive weighing of interests. This proportionality test should be mainly a task for national judges, as the conditions to be met are a matter for national law.

But some general guidelines may be taken from Article 8, paragraph 3, of the EU Copyright Directive, and the case law of the CJEU. Of importance are: intensity of the risk, commercial advantage of the hosting provider from the infringement, weighing of interests of copyright holder and host provider, expense of limiting risk of infringement, or lack of or existing possibilities to stop infringement. This means that the threshold of what is proportionate rises the more a hosting provider, through his behaviour, encourages rights infringements by third parties, for example by advertising using illegally-hosted content or setting up categories susceptible to infringement. Often, the perpetrators are anonymous, meaning

---

44 Case C-324/09 ¶ 136, 139, 141, *L’Oréal*.
45 *Id.* ¶ 135.
46 See Nordemann, *supra* note 27, ¶ 39 (with further references from German law).
47 See Bundesgerichtshof [BGH] [Federal Court of Justice], Cybersky, file no. I ZR 57/07, Jan. 15, 2009, MMR 625, 626 et seq. (2009); Oberlandesgericht [OLG] [Higher Regional Court] Hamburg, file no. 5 U 113/07, ZUM-RD 246 (2009); Oberlandesgericht [OLG] [Higher Re-
efficiently combating them is only possible via the host and not possible if each perpetrator has to be prosecuted individually.48

One must also take into account whether the hosting provider receives a consideration for the infringing acts. On the one hand, this covers cases in which the provider receives a financial benefit directly attributable to the infringement, in a case in which the provider has the right and ability to control the infringing activity. According to recent U.S. case law, “control” may require knowledge of the specific infringement. Pursuant to Section 512(c) of the U.S. DMCA, the provider loses its safe harbor in such scenarios. Also under EU law, in such cases the provider should be liable as an infringer and not only due to helping duties under Article 8, paragraph 3, of the EU Copyright Directive; in particular the provider should be liable for damages. On the other hand, there are other scenarios in which the provider generates direct or indirect profit through the infringement, but has no control. In such cases, the provider may come under the liability privilege of Article 14 of the EU E-Commerce Directive the same as it may qualify for the U.S. DMCA safe harbor. But even in such scenarios, the provider under EU Law may have non-contribution-based helping duties to act resulting in injunction claims against the provider in case it does not help (see III. 2.). Here, financial advantages can influence what measures are proportionate for the provider to implement under its duty to help. This is particularly true if the provider indirectly profits through increased advertising revenue due to the illegal act. For example, the income of advertising-financed hosting providers such as link referrers, file hosts and link encrypters rises with the number of times the hosted content is illegally accessed. Such providers should face increased helping duties, if they are not already liable as infringers.

When assessing the reasonableness of specific measures, one must not forget that a combination of measures could be most efficient. The following measures can be taken into account:49

- Notice to users to refrain from infringements;
- Hash value filters;
- Deletion interface. According to one of the more recent decisions of the Bundesgerichtshof (BGH), Kinderhochstuehle im Internet (children’s high chairs on the Internet), a deletion interface meets the duty of care to provide a search function to the right-holder which enables the latter to search with the same effort and success as the host provider. In a trademark case concerning eBay, eBay’s offer to the right-
holder to participate in eBay’s VeRI Programme was deemed sufficient.\textsuperscript{50} But offering right-holders the possibility of using a deletion interface is also insufficient as it cannot hinder the infringement as such, but simply provides the right-holder with the means to swiftly stop the infringement. In L’Oréal \textit{v.} eBay, the CJEU confirmed the duty of eBay to filter, even though L’Oréal had turned down eBay’s offer to use its VeRI Programme.\textsuperscript{51}

- **Keyword filters and other text-based due diligence measures.** Keyword filters do not breach the principle that providers must not be obliged to generally monitor their content (Article 15 of the EU E-Commerce Directive). In \textit{Netlog}, the CJEU held that all filtering duties that apply indiscriminately to all users as a preventive measure at the expense of the host provider and for an unlimited period of time breach Article 15 of the EU E-Commerce Directive.\textsuperscript{52} This does not mean that word filters may not be imposed on hosting providers. Word filters by their nature only search for certain film titles, game titles, audio book titles, music titles, band names etc. Also, they only filter the keywords belonging to the filed stores but not the file itself;

- **Audio and audio-visual filters.** These are offered by a number of manufacturers and are constantly improved. However, hosting providers are not obliged to use such filters on all content uploaded by any user, as this would result in a general monitoring duty. Such a filtering cannot be requested from the provider, as held in \textit{Netlog}.\textsuperscript{53} But the provider may voluntarily install it. What a provider may be obliged to install are audio-visual filters only for certain works upon knowledge that such works were made publicly available on the site. This is for example true for YouTube and its ID-Content-Filter system;\textsuperscript{54}

- **Manual controls.** Insofar as automatic filter procedures have gaps and cannot rule out rights infringements, these must be dealt with manually.\textsuperscript{55}

- **De-anonymizing infringing users.** Monitoring one-time infringers seems to be another effective measure. It is likely that one-time infringers will commit a similar rights infringement in the future. Thus, eBay is obliged to identify one-time infringers and terminate the accounts of repeat infringers.\textsuperscript{56} In order to identify repeat infringers, German case law demands, in part, the de-anonymization of rights-

\textsuperscript{50} See Bundesgerichtshof [BGH] [Federal Court of Justice], Kinderhochstuehle im Internet, file no. I ZR 139/08, July 22, 2010, GRUR 152 n.43 (2011).


\textsuperscript{52} Case C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) \textit{v.} Netlog NV (2012), [2012] C.M.L.R. 18.

\textsuperscript{53} \textit{Id}.


\textsuperscript{55} Bundesgerichtshof [BGH] [Federal Court of Justice], Internet-Versteigerung II, file no. I ZR 35/04, Apr. 20, 2012, GRUR 708 n.47 (2007); Jan Bernd Nordemann, in \textit{FROMM & NORDEMMANN}, supra note 18, sec.97 n.162.

\textsuperscript{56} Case C-324/09 \& 142, L’Oréal.
infringing users, in case there is no mandatory registration under a clear name. 57

From the U.S. perspective, it may be interesting that Section 512(i) of the U.S. DMCA requires the provider to take only limited preventive measures. The provider must adopt and reasonably implement a termination policy towards repeat infringers, if the providers want to profit from the DMCA’s safe harbors. EU law goes beyond this and also requires in particular content filtering duties besides repeat infringer termination policies. The reasons for such more extensive duties seem to be rooted in the different reasoning for the intermediary’s duties under EU law: They have to help because they are best placed to help (see above II. B.). Such duties to help have to be seen in contrast to the U.S. concept, which seems to be contribution-based.

IV. REMEDIES AGAINST ACCESS PROVIDERS (MERE CONDUITS)

Access providers usually provide Internet users with access and transmission services with respect to the Internet. They are also called “mere conduits.”

A. Liability Privileges of Access Providers (Article 12 of the EU E-Commerce Directive)

While the U.S. DMCA provides for safe harbors for ISPs that are engaged in “transitory network communication” in Section 512(a), Article 12 of the EU E-Commerce Directive stipulates that the national legislatures must establish liability shields for mere conduits. These liability shields in EU law also cover claims for copyright infringement, yet only cover damages and criminal liability. The privilege does not apply to claims for injunctive relief (see above II.B).

B. Injunction Claims Against Access Providers

Injunction claims against access providers may be granted pursuant to Article 8, paragraph 3, of the EU Copyright Directive irrespective of any liability of the access provider: “Member states shall ensure that right-holders are in a position to apply for an injunction against intermediaries

57 Oberlandesgericht [OLG] [Higher Regional Court] Hamburg, Rapidshare II, file no. 5 U 111/08, Sept. 30, 2009, MMR 51, nn.91 et seq. (2010) (in juris edition); see also Oberlandesgericht [OLG] [Higher Regional Court] Hamburg, Rapidshare I, file no. 7 W 69/08, July 8, 2009, ZUM-RD 527, 543 (2008); for a decision ruling against the possibility of identification via IP-addresses, see Oberlandesgericht [OLG] [Higher Regional Court] Düsseldorf, Rapidshare, file no. I-20 U 166/09, Apr. 27, 2010, ZUM 600, 603 (2010).
whose services are used by a third party to infringe a copyright-related right.” The CJEU confirmed this in several decisions starting with *LSG v. Tele2*,58 and in particular in *Scarlet v. SABAM*.59 Referring to the hosting provider decision *L’Oréal v. eBay*, the CJEU emphasised that also under Article 8, paragraph 3, of the EU Copyright Directive, access providers do not only have to bring to an end infringements, but they must also prevent further infringements:

Next, it follows from the Court’s case-law that the jurisdiction conferred on national courts, in accordance with those provisions, must allow them to order those intermediaries to take measures aimed not only at bringing to an end infringements already committed against intellectual-property rights using their information-society services, but also at preventing further infringements.60

In this respect, there seems to be a relevant difference to U.S. law. The DMCA in principle does not allow injunction claims against mere conduits if they are in the safe harbor.

But in the EU, the legal situation remains complex, as not all questions have been answered. The CJEU restated that the rules for the operation of the injunctions under Article 8, paragraph 3, of the EU Copyright Directive, such as those relating to the conditions to be met and to the procedure to be followed, are a matter for national law.61 This will cause some differences in the national case law across Europe. But there are some further principles that may be established on the EU level.

Access providers are gate keepers to any traffic by its subscribing customers. Hence, one possible measure to ask from access providers is to filter their traffic for illegal copyrighted content. Due to a reference of a Belgian Court, the CJEU in *Scarlet v. SABAM*62 ruled on filtering obligations, in particular for infringing peer-to-peer content in respect to SABAM’s entire repertoire as a Belgian musical collecting society. The CJEU held that imposing a filtering system to prevent copyright breaches for music and film files (1) that applies indiscriminately to all users, and (2) as a preventive measure, and (3) exclusively at the expense of the access provider, and (4) for an unlimited period, would be contrary to EU law. In particular, it would not be in line with Article 15 of the EU E-Commerce Directive, which prohibits an imposition of general monitoring duties of providers. *Scarlet v. SABAM* defines the limit for duties of access

---

60 *Id.* ¶ 31.
61 *Id.* ¶ 32.
62 *Id.* ¶ 54.
providers in the need to be specifically designed to stop infringement. To monitor all Internet traffic going through its infrastructure would push copyright protection too far.

But less far-reaching measures of access providers are possible. In particular, access providers could block certain Web sites pursuant Article 8, paragraph 3, of the EU Copyright Directive. Certain Internet sites have made it their business model not to respect the European legal framework. In particular, they make copyrighted works publicly available without the consent of the right-holder; also youth protection rules are not kept. Such structurally-infringing sites (also called “rogue” sites) usually cannot not survive in the EU because law enforcement would act against them quickly. Hence, such structurally-infringing sites operate anonymously and utilize hosting providers in “safe” countries, where the hosting provider will not follow the European rules for hosting-provider liability and duties (see above II.C).

One major example was the anonymously operated, German-language Web site kino.to, which made tens of thousands of movies publicly available without any consent by or remuneration to right-holders. Before the anonymous German operators were discovered in German criminal proceedings in the spring of 2011 and the site went down, kino.to was hosted in Russia; the hosting provider did not respond to NTD-letters and the Russian law enforcement authorities were unwilling to act. In the case of such structurally infringing sites, right-holders have raised claims against access providers in the EU to block access to such sites. Possible blocking measures are DNS-blocks, IP-address blocks, URL-blocks and combinations thereof.

With respect to such Web site blocking claims, further guidance will be provided from a CJEU ruling that can be expected in 2013. The Austrian Oberster Gerichtshof (OGH) has referred several questions to the CJEU, after lower level courts had granted Web site blocking orders with respect to kino.to against an Austrian access provider.63 The OGH first thought that it was not entirely clear from Article 8, paragraph 3, of the EU Copyright Directive if the services of an access provider are used in case the customers of the access provider access a Web site with infringing content. In particular in respect of the making available right, it is sufficient for the infringement, if the work offered to the public. Strictly legally speaking, the reception by the access provider’s customer is not necessary. But the OGH rightly argued in favour of a use of the provider’s services nevertheless. The making available only makes economic sense, if there

---

63 Oberster Gerichtshof [OGH] [Supreme Court], file no. 4 Ob 6/12d, May 11, 2012. At the CJEU, the case has the file no. C-314/12 – UPC-Telekabel Wien.
are Internet users who are the recipients.\textsuperscript{64} Also, it has to be borne in mind that use of the making available right (also) takes place in the country of reception.\textsuperscript{65}

Otherwise, one would have to look at the question of whether Internet users downloading or streaming from the Web site infringe copyright themselves. Thus, the Austrian court consequently wanted to also know, if a legal reproduction for private use (Article 5, paragraph 2 lit. b, of the EU Copyright Directive) and a transient and integral reproduction (Article 5, paragraph 1, of the EU Copyright Directive) require that the source for the reproduction has been legally reproduced, distributed or made available online.

But the crucial issue about Web site blocking claims remains the proportionality test. The OGH explicitly requested “guidelines” from the CJEU with respect to the proportionality test.\textsuperscript{66} In general, the proportionality test will require a case-by-case analysis weighing all quantitative, but also all qualitative aspects: in particular fundamental rights such as the guarantee of intellectual property (Article 17, paragraph 2, of the Charter of Fundamental Rights of the European Union); the freedom to conduct a business enjoyed by operators, such as access providers pursuant to Article 16 of the Charter; and fundamental rights of that access provider’s customers, namely their right to protection of their personal data and their freedom to receive or impart information, which are rights safeguarded by Articles 8 and 11 of the Charter respectively.\textsuperscript{67} More specifically, the following questions will come up.

One major issue is the effectiveness of the blocking measures. The OGH asked the following question: Does it conform with EU law, in particular with the required assessment and balance between fundamental rights of all persons involved, that an access provider is ordered to introduce specific measures in order to impede its clients access to a Web site with content made available online without consent, \textit{if} these measures are not-insignificantly costly, but can also easily be circumvented without specific technical knowledge? Specifically, the Austrian court thought that alternative sites such as kinox.to, which emerged after the takedown of kino.to, would show that Web site blocking could be ineffective. However, it seems to be necessary to take a more sophisticated look at circumvention. For example, the question asked by the OGH seems to be too narrowly construed, as it is merely directed toward the technical feasibility of

\textsuperscript{64} Oberster Gerichtshof [OGH] [Supreme Court], file no. 4 Ob 6/12d, at 8.
\textsuperscript{65} See supra II.C.
\textsuperscript{66} Oberster Gerichtshof [OGH] [Supreme Court], file no. 4 Ob 6/12d, at 24.
circumvention. But most consumers will not use circumvention tools technically available.

Polls in Member States such as Germany have shown that a larger majority of internet users will not use circumvention technically possible if they are made aware that the content available is illegal. Also, for “well-known trademarks” among the rogue sites, such as thepiratebay.org, evasion to other domains can mean a considerable loss in users. Furthermore, it must influence the proportionality test, that in cases as described above, Web site blocking remains the only tool to at least impede infringements by such “rogue” sites. The CJEU emphasised multiple times that it is necessary to strike a “fair balance” between all fundamental rights in question, which implies that intellectual property pursuant to Article 17, paragraph 2, of the Charter of Fundamental Right of the European Union must not be left without any protection. Article 8, paragraph 3, of the EU Copyright Directive is of paramount importance in particular, where individual action fouls for whatever reason.

Further guidance for the proportionality test comes from case law in EU-Member States. So far there have been two decisions come from the British High Court of Justice’s Chancery Division: on 28 July 2011 (Newzbin2 I) and on 26 October 2011 (Newzbin2 II). In Newzbin2 I, British Telecom was obligated to block access to the site newzbin2, a Web site that mainly made films, music and computer games available to the public unlawfully. The decisions of the British High Court of Justice were based on Article 97a and Article 191JA of the British Copyright Designs and Patent Act 1988 that implemented Article 8, paragraph 3, EU Copyright Directive. In the Approved Second Judgment Newzbin2 II, it was specified that British Telecom was to implement the Cleanfeed process (roughly speaking a combination of IP address filtering and URL blocking) for the access block.

In Great Britain, blocking structurally infringing Web sites has become an established practice of the relevant Internet access providers there (not only British Telecom) as a result of this decision. The extensive

---

68 See Case C-461/10 ¶ 56, Bonnier Audio AB v. Perfect Communication Sweden AB (Jan. 29, 2008), EUR-Lex; Case C-275/06 ¶¶ 68-70, Productores de Música de España (Promusicae) v. Telefónica de España (Jan. 29, 2008), EUR-Lex.


70 Twentieth Century Fox Film Corp. v. British Telecommunications, plc, [2011] EWHC 1981 (Ch.).

71 Twentieth Century Fox Film Corp. v. British Telecommunications, plc, [2011] EWHC 2714 (Ch.).

72 Id. ¶ 56.
and well-argued British High Court of Justice decision, *Newzbin2 I*, explores in great detail the proportionality of Web site blocking claims. Here, in particular the “spill-over effect” became relevant. With respect to legal content, which may be available on the Web site and will be blocked, the British High Court of Justice applied a “de minimis” test. As *Newzbin2* contained over 90% unlawful content, the legal content was irrelevant.73 In result, this seems to be convincing. It must speak in favour of blocking, if the Web site follows an illegal business model (which is the case with more than 90% illegal content) or advertises illegal use of its content.

The “spill-over effect” on illegal content should be irrelevant from the start, if — as usually — only some right-holders sue in respect to a part of the work illegally made available on the Web site. This should be at least true, if there are no hints that the other right-holders would not be supportive. The High Court said:

> It is true that the order sought will also benefit other rightholders, but I do not regard this as a reason for refusing the order. On the contrary, I consider that it supports the making of the order. . . . [T]here is no reason to believe that they would not be equally supportive of the application.74

Case law from other EU-Member States confirms that proportionate claims for Web site blocking are possible. A decision from the Danish Supreme Court allowed Web site blocks (in the form of DNS-blocks) with respect to the vastly illegal Web site, *thepiratebay.org*.75 In Belgium, the Court of Appeal Antwerp on 26 September 2011;76 and in the Netherlands, the Dutch Rechtsbank at the Hague on 11 January 2012,77 have issued injunctive orders for Web site-blocking, all relying on the respective national implementation of Article 8, paragraph 3, of the EU Copyright Directive.

In Germany, claims by right-holders to block such “rogue” sites have led to some decisions under the German doctrine of *Störerhaftung* with respect to Internet access providers that, according to this doctrine, have a duty to prevent copyright infringements after they become aware of thereof.78 But German courts struggled with the national implementation of Article 8, paragraph 3, of the EU Copyright Directive. Some German

---

73 *Id.* ¶ 52.
74 Twentieth Century Fox Film Corp., [2011] EWHC 1981 ¶ 185 (Ch.).
75 File no. 153/2009 (May 27, 2010).
76 File no. 3399-2011/8314 (Sept. 26, 2011).
78 Oberlandesgericht [OLG] [Higher Regional Court] Hamburg, Usenet I file no. 5 U 113/07, Jan. 14, 2009, ZUM-RD 246, 257 (2009); Oberlandesgericht [OLG] [Higher Regional Court] Frankfurt am Main, Auskunftsanspruch, file no. 11 U 51/04, Jan. 25, 2005, GRUR-RR 147, 148 (2005); Landgericht [LG] [Regional Court] Hamburg, file no. 308 O 548/08, Nov. 12, 2008, ZUM
courts were reluctant to grant Web site blocking orders under the doctrine of Störerhaftung.

The most prominent case concerned the request for blocking the Web site g-stream.in, which is a site prevalently providing links to infringing content. Its operators are unknown, and the Web site is hosted in Russia; the host provider does not react to notice and takedown requests from right-holders. The OLG Hamburg in a recent decision refused to grant a Web site-blocking order even in the light of Article 8, paragraph 3, of the Copyright-Directive. The court argued that the German legislature had not sufficiently implemented Article 8, paragraph 3, of the Copyright-Directive. The court thus did not find itself in a position to grant such Web site blocking orders only in the light of Article 8, paragraph 3, of the EU Copyright Directive without a specific, detailed national German law.

In a recent preliminary ruling, the OLG Cologne, however, did not follow the OLG Hamburg’s approach. In light of Article 8, paragraph 3, of the EU Copyright Directive, the Cologne judges expressed the opinion that in principle injunction claims also under German law would be possible, if the claim is proportionate. Consequently, also in German law, it all comes down to a proportionality test, as before the CJEU in respect to blocking the Web site kino.to already mentioned above.

C. Information Claims Against Access Providers

Many consumers — although the number is declining — make copyright-protected music, films or audio books publicly available on the Internet in so-called peer-to-peer networks. These peer-to-peer networks are also publicly accessible for investigators of right-holders. However, the right-holders are limited to finding out the IP-address which was used for the illegal upload to the peer-to-peer network. This IP-address has to be matched with the provider’s customer data at the Internet access provider the infringing consumer used for the illegal upload. In the case of so-called static IP-addresses, which are always used by the same consumer, the provider will be able to identify his customer by merely matching the IP-address with the customer’s name. In most of the cases, however, access providers provide their customers with so-called dynamic IP-addresses,

587, 589 (2009); see also Nordemann, in FROMM & NORDEMANN, supra note 1, section 97 n.170.


80 Oberlandgericht [OLG] [Higher Regional Court] Cologne, file no. 6 U 192/11, Apr. 20, 2012 preliminary ruling (“Hinweisbeschluss”).
which can change with each of the consumer’s sessions. Therefore, identification of the relevant consumer requires both the dynamic IP-address and the exact time at which the IP-address was used.\textsuperscript{81}

Therefore, right-holders are looking to raise information claims against an access provider to identify a customer. Article 8 of the Enforcement Directive provides for such an information claim. But such an information claim produces certain tensions regarding the fundamental rights of third parties. Here, the CJEU has taken a balancing position. According to the Court, Article 8 of the Enforcement Directive, read in conjunction with Article 15, paragraph 1, of the Directive on Privacy and Electronic Communications,\textsuperscript{82} does not preclude Member States from imposing an obligation to disclose to private persons personal data in order to enable them to bring civil proceedings for copyright infringements, but nor does it require those Member States to lay down such an obligation.\textsuperscript{83} Therefore, it is of no surprise that the implementation in the EU-Member States has produced different models.

In Germany, Section 101 of the Copyright Act (“UrhG”) allows information claims of the right-holder against the Internet access provider under civil law to identify infringing customers by separate court order. It is a pre-requisite that there is an obvious right of infringement, or that the infringed party has already instituted proceedings against the infringer. Section 101 paragraph 9, of the UrhG also compels Internet access providers to provide information when they allocate dynamic IP-addresses for the access of their customers, i.e., in cases in which IP-addresses are not constantly allocated to the same customer but the Internet access provider allocates a new IP-address for each of the customer’s new Internet sessions.

In that regard, a special judicial procedure can be found in Section 101, paragraph 9, of the UrhG, which must be undertaken before the Internet access provider may identify the customer to the right-holder, using a dynamic IP-address. The reasons for this lie in the fact that the German

\textsuperscript{81} Beyond peer-to-peer networks, the identification of the infringing consumer is usually irrelevant; for example, this is true for platform piracy (such as the “rogue” Web site described above), where consumers are “only” streaming or downloading. Streaming or downloading can also be a breach of copyright, i.e., of the (temporary) reproduction right, but usually it is not pursued by rights holders.

\textsuperscript{82} 2002/58/EC.

legislature feared that in the absence of a judicial order, there could be a violation of the constitutionally guaranteed privacy of telecommunication. The costs for the court proceedings required are borne by the infringed party and not by the Internet access provider (Section 101, paragraph 9, sentence 5, of the UrhG). The right-holder can, however, claim the costs as compensation from the infringing customer provided the customer is able to pay. In contrast to what was held by some lower level courts in Germany, there is no requirement in Section 101 of the UrhG that the infringement must have been committed on a “commercial scale,” rather, in principle, even small infringements also qualify for an information claim.

Since the introduction of this right to information as of September 1, 2008, it has been extensively used (with thousands of cases every month) by right-holders from the music industry and some from the film industry against Internet access providers to force them to identify their rights-infringing customers. Consumers have to pay cost-reimbursement for attorney fees, court fees and damages, which usually results in payment from €400 to €2,000.

In German copyright law, the information claim of right-holders against Internet access providers (“ISPs”) for the identification of infringing Internet users faces some limitations. This poses a particular problem for the right-holder in cases in which the infringer may only be identified through a successful information claim; e.g., in peer-to-peer scenarios. This is particularly true due to insufficient data available at the access provider to fulfill the information claim. Data retained due to the EU-Data Retention Directive (2006/24/EC) may not be used to satisfy the information claim, but only so-called billing data.

With respect to the availability of data, ISPs may be separated into three categories:

- ISPs retaining data for seven days (no ISP in Germany retains data longer than this). Here, although a considerable speed of the right-holder is necessary, efficient enforcement is possible;
- A second category of ISPs retain the data for only a very limited number of days, e.g. for two days. This time is so short that the right-holder “loses” a considerable number of cases (example: infringement Friday, data deleted on Sunday);

---

86 Now confirmed by the BVerfG [German Constitutional Court], decision of March 2, 2010, file no. 1 BvR 256/08, NJW 833 (2010).
Internet Copyright Infringement

- A third ISP category does not retain data at all. Some courts — like the Regional Court (Landgericht, LG) Hamburg\(^{87}\) — have granted orders to right-holders obliging the ISPs to freeze the deletion of retained data on a mere “call” by the right-holder during the Internet session of the infringing internet user. Other courts have rejected such “freezing orders.”\(^{88}\) In general, German courts only have jurisdiction for those ISPs that have their seat or branch in the court’s district. The inhomogeneous case law on “freeze orders” has the result that some ISPs have to face “freezing orders,” as the court of their company seat or branch is in favour of such orders, while other ISPs with their seat in a different district court will not. As a result, Frankfurt-based ISP Arcor (Vodafone Group) and Düsseldorf-based ISP Vodafone may never be the target of successful information claims and thus infringers using, e.g., Arcor’s and Vodafone’s Internet access may never be pursued by a right-holder.

In France, a state institution called “HADOPI”\(^{89}\) raises the information claims against access providers. Afterwards, a “graduated response” model applies: HADOPI sends warnings to the owners of infringing accesses. After the third warning, measures may be taken by HADOPI, e.g., to order the temporary cutting off of Internet access. HADOPI has sent several hundred thousand warnings on the first level, but only a few hundred warnings on the third level.

In Great Britain, a civil law procedure has been chosen by the Digital Economy Act 2010.\(^{90}\) Right-holders raise information claims against access providers and a “graduated response” model applies: It provides for a duty on access providers to forward notifications of infringement to their customers. On request by the right-holder, access providers also have to provide an anonymized list of notifications received with respect to a given account. On application by the right-holder under the Norwich Pharmacal jurisdiction,\(^{91}\) the court may order the access provider to disclose the identity of its customer; to enable the right-holder to bring proceedings. The implementation the Digital Economy Act is under the control of the British regulator (OFCOM). The system is not in operation yet (expected for early 2014).


\(^{88}\) Oberlandesgericht [OLG] [Higher Regional Court] Frankfurt, file no. 11 W 41/09, Nov. 12, 2009, MMR 62 (2010); see also the Düsseldorf courts.


\(^{91}\) Norwich Pharm. Co. v. Customs & Excise Comm’rs, [1974] AC 133.
V. SUMMARY

- The liability shields in Articles 12 to 14 EU E-Commerce Directive apply to copyright infringement claims, but — in contrast to the U.S. DMCA — only cover in particular damages and criminal liability. They do not cover injunction claims. Article 8, paragraph 3, of the EU Copyright Directive requires the national legislature to provide for injunction claims against “intermediaries” whose services are used for copyright infringements irrespective of any liability. Both hosting providers and access providers are “intermediaries” in that sense. The reason why injunction claims may be raised against them is the fact that they are in a good position to help. This is comparable — to a certain extent — to helping duties existing in the general civil law of the Member States.

- With respect to hosting providers, the CJEU ruling, L’Oréal v. eBay sets the standard. Similar to the U.S. DMCA, hosting providers can rely on the liability defence of Article 14 of the EU E-Commerce Directive if they take a “neutral” position as to users’ content. Furthermore, they must not be aware of facts or circumstances from which illegality is apparent. The CJEU held that the “diligent economic operator” is the standard. With respect to injunction claims, hosting providers, after they have been notified of any infringement, have to ensure that they do not only bring an end to infringements by a user, but also prevent further infringement of that kind. In contrast to U.S. law, such preventative measures are not limited to termination duties with respect to repeat infringers. Prevention duties can also consist of filtering measures, which must, however, be proportionate. Following the CJEU Netlog ruling, a filtering of all content may not be asked for.

- For access providers (mere conduits), the case law of the CJEU is less refined, but prevention duties have been confirmed by the CJEU in Scarlet v. SABAM even if the mere conduit qualifies for the liability privilege. This is different from U.S. law, but the Scarlet v. SABAM ruling has only set the outer limit for injunction claims, which may not oblige the provider to filter all of its traffic. With respect to Web site blocking (in particular blocking of structurally infringing sites hosted “safely” abroad), which would not use such filters, the CJEU decision UPC Telekabel Wien (kinoto) is eagerly awaited. This decision will in particular clarify the general standards for the necessary proportionality test. Here, it should be taken into account that such blocking claims re-
main the only remedy for the right-holder to impede infringements.

EXHIBIT: RELEVANT PROVISIONS OF EU LAW:

EU Copyright Directive:

Article 8
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.

Recital 59:
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, . . . rightholders should have the possibility of applying for an injunction . . . . This possibility should be available even where the acts carried out by the intermediary are exempted under Article 5. The conditions and modalities relating to such injunctions should be left to the national law of the Member States.

EU E-Commerce Directive:

Article 12 “Mere conduit”
1. 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.
2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.
3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States’ legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 13 “Caching”
1. 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, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more effi-
cient the information’s onward transmission to other recipients of the service upon their request, on condition that:
(a) the provider does not modify the information;
(b) the provider complies with conditions on access to the information;
(c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
(d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
(e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States’ legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 14 Hosting
1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States’ legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

Article 15 No general obligation to monitor
1. Member States shall not impose a general obligation on 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.

2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.