

Secondary Liability for Trademark Infringement on the Internet: The Situation in Germany and Throughout the EU

Annette Kur*

I. LEGAL BACKGROUND

It is a safe assumption¹ that every one of the twenty-eight EU Member States has some form of secondary liability principles within its general tort law. Traditionally, tort law principles require an element of deliberate contribution to, and therefore positive knowledge of, another person's action. They are therefore of limited value for situations like Internet infringement, because the contributor is typically unaware of persons committing concrete acts of infringement. When the contributor merely provides the technical infrastructure that is used by an anonymous crowd for legitimate as well as illegitimate purposes, the "deliberate contribution" or "positive knowledge" element is difficult to prove.

The general principles of tort law are not harmonized within Europe.² However, regarding Internet services that may be misused for unlawful acts (including, but not limited to, intellectual property infringement), the E-Commerce Directive has created a legal framework for exemptions from liability (the safe harbor).³ In that regard, the E-Commerce Directive is the European equivalent of the U.S. Digital Millennium Copyright Act (DMCA), with the notable distinction that the E-Commerce Directive applies horizontally, thus encompassing trademark infringement. Articles 12 through 14 of the E-Commerce Directive stipulate that, regarding transmission, caching and hosting, no liability will ensue if the person

* Senior Research Fellow, Max Planck Institute for Intellectual Property and Competition Law.

1. It is not clear whether this particular aspect has ever been investigated in a comparative study covering all twenty-eight EU Member States.

2. Preparatory work on harmonization and unification of European Civil Law was commenced in the 1980s by a group of scholars formed around the Danish professor Ole Lando (the Lando Commission) and was later continued by several academic groups. Two of them, the Study Group on a European Civil Code and the Research Group on EC Private Law (Acquis Group), prepared a Draft Common Frame of Reference (DCFR) in 2009. See STUDY GRP. ON A EUROPEAN CIVIL CODE & RESEARCH GRP. ON EC PRIVATE LAW (ACQUIS GRP.), PRINCIPLES, DEFINITIONS AND MODEL RULES OF EUROPEAN PRIVATE LAW (2009), available at http://ec.europa.eu/justice/policies/civil/docs/dcfr_outline_edition_en.pdf. The DCFR contains a chapter on non-contractual liability, but the emphasis is on issues of contract law. See *id.* The report led to a European Commission proposal for a Regulation on a Common European Sales Law (CESL). *Commission Proposal for a Regulation of the European Parliament and of the Council on a Common European Sales Law*, SEC (2011) 1165 final (Oct. 11, 2011).

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, 2000 O.J. (L 178) 1–16 [hereinafter E-Commerce Directive].

rendering such services: (1) confines his or her role to enabling use by others; and (2) reacts expeditiously upon receiving information about illegitimate content.⁴ Article 15 sets forth explicitly that Internet service providers (ISPs) acting within the limits prescribed in Articles 12 through 14 have no obligation to monitor content proactively.⁵ The directive does not spell out the consequences for ISPs that do not comply with those rules. The legal grounds on which they are eventually held liable, and whether liability is for secondary or primary infringement, are to be determined by national law.⁶

A second act of EU legislation relevant to secondary liability is the Enforcement Directive.⁷ Articles 11 and 8(1)(c) of the Enforcement Directive stipulate that Member States may issue permanent injunctions and grant requests for third-party information against those providing commercial services that are used for an infringement.⁸ Again, the Directive does not specify further the legal grounds on which liability shall rest.

As the legal interest in pursuing infringers increasingly turns towards intermediaries, it is frequently necessary for courts to decide cases that address the principles set out in the E-Commerce and Enforcement Directives. As yet, it is still difficult to obtain a complete picture of current legal practices in the Member States.⁹ Although the decisions rendered by the Court of Justice of the European Union (CJEU) have not substantially alleviated the law's obscurity, some basic principles can be derived from the court's case law. Generally speaking, the CJEU is cautious when the interests of intellectual property owners are pitched against

4. *Id.* at 12–13.

5. *Id.* at 13.

6. For more details, see Graeme B. Dinwoodie, *Secondary Liability for Online Trademark Infringement: The International Landscape*, 37 COLUM. J.L. & ARTS 463 (2014).

7. Council Directive 2004/48/EC, on the Enforcement of Intellectual Property Rights, 2004 O.J. (L 157) 45–86 [hereinafter Enforcement Directive].

8. Article 11 states, “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 an intellectual property right, without prejudice to Article 8(3) of Directive 2001/29/EC [the Copyright Directive].” *Id.* at 76. Under Article 8(1)(c),

Member States shall ensure that, in the context of proceedings concerning an infringement of an intellectual property right and in response to a justified and proportionate request of the claimant, the competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided by the infringer and/or any other person who . . . was found to be providing on a commercial scale services used in infringing activities.

Id. at 67–68. The wording of Article 8(3) of Directive 2001/29/EC is the same as the third sentence of Article 11 of the Enforcement Directive, but for the fact that it refers to copyright and related rights instead of IP in general. See 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, 2001 O.J. (L 167) 10.

9. For comparative accounts of legal practices in select EU countries, see Rita Matulionyte & Sylvie Nérissou, *The French Route to an ISP Safe Harbour, Compared to German and US Ways*, 42 INT'L REV. OF INTEL. PROP. & COMPETITION L. 55 (2011); Matthias Leistner, *Common Principles of Secondary Liability?*, in COMMON PRINCIPLES OF EUROPEAN INTELLECTUAL PROPERTY LAW 117–46 (Ansgar Ohly ed.). See also Dinwoodie, *supra* note 6.

those of ISPs.¹⁰ The CJEU emphasizes the principle—enshrined in Article 15 of the E-Commerce Directive—that ISPs should not be subject to a general monitoring obligation,¹¹ and several decisions have called for a fair balance between efficient enforcement of IP rights and countervailing values, such as the freedom to conduct a business,¹² protection of private data¹³ and other fundamental rights.¹⁴ However, the CJEU took a stricter position regarding the conditions under which ISPs can avail themselves of the safe harbor clauses in the E-Commerce Directive, stating that liability might be triggered by any kind of active involvement in shaping content.¹⁵

Due to the uncertainties prevailing in the patchwork structure of current EU law, this Article does not undertake to provide a comprehensive account of the pertinent problems and solutions throughout Europe. Instead, the presentation focuses on German law, where the mechanism of *Störerhaftung* (the liability of a *Störer*, meaning “disquieter” or “interferer”) has attracted some attention in other Member States.¹⁶

This Article will address cases in which ISPs face liability without directly committing an allegedly infringing act. It will then discuss whether, and under what conditions, ISPs may be held liable (for primary infringement or otherwise) under the safe harbor rules in the E-Commerce Directive. The following section expands on the notion of *Störerhaftung* in German law, explaining its origin, basic requirements and contentious features. The operation of the *Störer*-mechanism will be illustrated by reference to case law, in particular a recent series of decisions regarding the services of RapidShare. As those decisions concern copyright infringement, the conclusion addresses the extent to which they could have repercussions for issues of trademark infringement.

II. WHAT KIND OF INFRINGEMENTS ARE WE TALKING ABOUT?

As pointed out above, one obvious distinction between the U.S. and the EU approaches towards secondary liability is that the pertinent EU provisions apply horizontally: they do not distinguish between infringement of copyright, on the one hand, and other IP rights on the other. This means that legal practices and case law

10. For trademark law, this cautious attitude is reflected in particular in Joined Cases C-236/08–C-238/08, *Google France SARL v. Louis Vuitton Malletier SA*, 2010 E.C.R. I-02417.

11. Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011 E.C.R. I-11959, ¶ 40.

12. *Id.* ¶ 48; Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*, 2012 E.C.R. I-00000, 2 C.M.L.R. 18 (2012), ¶ 46, available at <http://curia.europa.eu/juris/document/document.jsf?docid=119512&doclang=EN>.

13. Case C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, 2008 E.C.R. I-271, ¶¶ 41, 68; Case C-461/10, *Bonnier Audio AB v. Perfect Communication Sweden AB*, 2012 E.C.R. I-00000, 2 C.M.L.R. 42 (2012), ¶ 59, available at <http://curia.europa.eu/juris/document/document.jsf?docid=121743&doclang=EN>.

14. Case C-360/10, *Netlog*, ¶¶ 41–43; Case C-70/10, *Scarlet*, ¶¶ 43–45.

15. Case C-324/09, *L’Oréal SA v. eBay Int’l AG*, 2011 E.C.R. I-6011, ¶¶ 115–116.

16. See *L’Oréal SA v. eBay Int’l AG*, [2009] EWHC (Ch) 1094, [455] (Arnold, J.) (Eng.).

developed with regard to copyright law are also basically applicable in the area of trademark law. Upon closer inspection, however, it may be that even in the EU, applicable standards and concerns in copyright cannot simply be transposed to trademark. Despite the common legal groundwork, the different considerations to be adjudicated might call for different reasoning in trademark cases.¹⁷

For a rough sketch of claims that seek to establish liability of ISPs in connection with trademark infringement, it may be appropriate to distinguish between two major types of infringement. The main characteristic of the first, “Google-type” cases, is that the direct infringers use third parties’ trademarks as a means to catch the attention of Internet users, and thereby increase traffic to their own Web sites.¹⁸ This will sometimes, but not necessarily, cause confusion about the actual source of communication. This type of infringement is rather novel and does not fit easily into the traditional structure of trademark law. It began with domain name grabbing,¹⁹ generated new phenomena such as metatagging²⁰ and is now most relevant in the context of keyword advertising.²¹ Keyword advertisements, where search engines offer to “optimize” the display of advertising by selecting trademarks as keywords, are frequently the bases of claims for secondary liability for this type of infringement.²² In domain name grabbing cases, secondary liability might be claimed against registrars or administrative contacts.²³ These cases have hardly any parallel in the context of copyright infringement; they appear to be trademark-specific.

The second type of case concerns sales of counterfeits (or goods otherwise

17. It may also be noted, in this context, that the German notion of *Störerhaftung* is regularly applied only in trademark and copyright law. In patent law, a narrower notion of tortious contributory liability applies. This schism in German jurisprudence may be due to the fact that indirect liability is explicitly regulated in Section 10 of the German Patent Act, but also reflects different attitudes prevailing in the German Federal Court of Justice chambers dealing with patents and with other IP rights, respectively. See generally Leistner, *supra* note 9, at 123–30.

18. See, e.g., Joined Cases C-236/08–C-238/08, *Google France SARL v. Louis Vuitton Malletier SA*, 2010 E.C.R. I-02417.

19. The issue was first raised in the 1990s and led, in the U.S., to specific legislation. Anticybersquatting Consumer Protection Act (ACPA), 15 U.S.C. § 1125(d) (2012). The Internet Corporation for Assigned Names and Numbers (ICANN) adopted the parallel Uniform Dispute Resolution Policy (UDRP). *Uniform Domain Name Dispute Resolution Policy*, INTERNET CORP. FOR ASSIGNED NAMES & NUMBERS, <http://www.icann.org/en/help/dndr/udrp/policy>.

20. See *Brookfield Commc’ns v. West Coast Entm’t Corp.*, 174 F.3d 1036 (9th Cir. 1999); *Playboy Enters., Inc. v. Netscape Commc’ns Corp.*, 55 F. Supp. 2d 1070, 1077 (9th Cir. 1999). In Germany, metatagging is considered to be infringing unless it can be justified by specific reasons. See Bundesgerichtshof [BGH] [Federal Court of Justice] May 18, 2006, GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT [GRUR] 65, 2007 (Ger.) (*Impuls*); Bundesgerichtshof [BGH] [Federal Court of Justice] Feb. 8, 2007, 9 GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT [GRUR] 784, 2007 (Ger.) (*AIDOL*). The CJEU has never addressed the issue of metatags in the context of trademark law.

21. See, e.g., *Google France*, 2010 E.C.R. I-2417.

22. See *id.*

23. Indirect liability of the so-called admin-c (administrative contact) registered with the domain name registry (in Germany, DENIC administering the TLD.de) has become a topic frequently addressed by German courts. For an overview of the resulting decisions, see Thomas Hoeren and Sonja Eustergerling, *Die Haftung des Admin-C: Ein kritischer Blick auf die Rechtsprechung*, 9 MULTIMEDIA UND RECHT [MMR] 132, 132–38 (2006) (Ger.).

infringing trademark rights) that are offered through Internet platforms on particular auction sites.²⁴ Unlike the previous category, there are no particular legal obstacles to classifying the direct acts committed by users of the ISP's services as infringement. Generally, the illicit character of knock-off goods can be taken for granted. These cases arguably bear some resemblance to the notorious issue of file-sharing Web sites for illegally reproduced content. However, unlike the issue presented by file-sharing and other cases of unauthorized Web sites that create access to copyrighted works, consumers cannot download counterfeits and other trademark-infringing goods directly from the Internet—the physical article needs to be shipped to the customer. Also unlike copyright infringements via unauthorized file-sharing Web sites, counterfeits are neither offered for free nor mutually exchanged among users in a general scheme of “sharing”; some payment will always be made.²⁵ Lastly and most importantly, while digital files of music, books or movies are reproduced at the click of a button, such that one illegal copy can become viral and engender millions of others, each individual counterfeit article must be produced by analog means in the analog world. All of this makes it less likely that intermediaries will develop business models specifically aimed at offering counterfeit articles.²⁶ Auction platforms or other virtual marketplaces usually flourish only if what is offered meets the demands of the customers, and while customers want to make a good bargain, they are not likely to be interested solely in fakes.

III. CONDITIONS FOR ESTABLISHING LIABILITY

A. PRIMARY VS. SECONDARY LIABILITY

Proposed secondary liability regimes suffer from a lack of established taxonomy separating the different forms of liability, which are not labeled in a universally accepted manner. There is no common understanding of what, exactly, is meant by “indirect,” “secondary,” “contributory” or “vicarious” infringement.²⁷ The line

24. That is, goods bearing signs that are similar to protected marks, without a close enough resemblance to classify as “counterfeit” in the meaning of footnote 14 to TRIPS Article 51. Agreement on Trade-Related Aspects of Intellectual Property Rights, art. 51 n. 14, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, THE LEGAL TEXTS: THE RESULTS OF THE URUGUAY ROUND OF MULTILATERAL TRADE NEGOTIATIONS 320 (1999), 1869 U.N.T.S. 299, 322 [hereinafter TRIPS Agreement]. Furthermore, due to the principle of so-called regional exhaustion, even sales of original goods would be considered infringements in the EU if the rights holder has only consented to marketing outside the EU.

25. Such payments leave traces that may assist the rights holder in tracking down the source of the infringement. In that context, it may be interesting to note that the German Federal Court of Justice has decided to refer to the CJEU the question of whether Article 8(3) of the Enforcement Directive requires a bank to disclose the name and address of a customer to whose account payments have been made for counterfeit articles, or whether the bank can invoke banking confidentiality as a defense under Article 8(3)(e). Case C-580/13, Request for a preliminary ruling from the Bundesgerichtshof (Germany) lodged on 18 November 2013, *Coty Germany GmbH v. Stadtparkasse Magdeburg*, 2014 O.J. (C 31) 4.

26. One possible exception is depersonalization services.

27. See Dinwoodie, *supra* note 6.

separating primary infringement from the diverse forms of secondary liability is also uncertain.

In the EU, the differences between the two depend on the specifics of national law. Nevertheless, EU law sets out some minimum requirements for finding primary trademark infringement by ISPs. Most importantly, any finding of trademark infringement under harmonized trademark law,²⁸ as well as under the Community Trademark Regulation (CTMR),²⁹ depends on whether the ISP has used the mark in the course of trade in a manner that affects or is likely to affect the trademark functions.³⁰ In part, this analysis assesses whether the alleged infringer has used the mark in its own commercial communication.³¹ That element was found not to have been met with regard to search engines (“referencing service providers”) operating a keyword advertising system; the CJEU found that:

[T]he referencing service provider operates “in the course of trade” when it permits advertisers to select, as keywords, signs identical with trade marks, stores those signs and displays its clients’ ads on the basis thereof, [but] it does not follow . . . from those factors that that service provider itself “uses” those signs [U]se, by a third party, of a sign identical with, or similar to, the proprietor’s trade mark implies, at the very least, that that third party uses the sign in its own commercial communication. A referencing service provider allows its clients to use signs which are identical with, or similar to, trade marks, without itself using those signs.³²

Similarly, with regard to auction platforms and other Internet marketplaces, the court found that:

In so far as [a] third party provides a service consisting in enabling its customers to display on its website, in the course of their commercial activities such as their offers for sale, signs corresponding to trade marks, it does not itself use those signs within the meaning of . . . EU legislation.³³

Consequently, national courts in the EU have no more room for examining whether ISPs such as Google or eBay are liable for direct trademark infringement: it must

28. EU trademark laws have been harmonized on the basis of the Trade Mark Directive. Council Directive 89/104, of 21 December 1988 to Approximate the Laws of the Member States Relating to Trade Marks, 1989 O.J. (L 40) 1–7 (EU) (original enactment); Directive 2008/95, of the European Parliament and of the Council of 22 October 2008 to Approximate the Laws of the Member States Relating to Trade Marks, 2008 O.J. (L 299) 25–33 (EU) (codified version).

29. Council Regulation 40/94 of 20 December 1993 on the Community Trade Mark, 1994 O.J. (L 11) 1–36 (EC); Council Regulation 207/2009 of 26 February 2009 on the Community Trade Mark, 2009 O.J. (L 78) 1–42 (EC) (codified version).

30. See, e.g., Case C-487/07, *L’Oréal SA v. Bellure NV*, 2009 E.C.R. I-5185, ¶¶ 58–65; Case C-48/05, *Adam Opel AG v. Autec AG*, 2007 E.C.R. I-1017, ¶¶ 16–37; Case C-206/01, *Arsenal Football Club plc v. Reed*, 2002 E.C.R. I-10273, ¶¶ 38–62.

31. See Case C-119/10, *Frisdranken Industrie Winters BV v. Red Bull GmbH*, 2011 E.C.R. I-13179, ¶ 30; Case C-324/09, *L’Oréal SA v. eBay Int’l AG*, 2011 E.C.R. I-6011, ¶ 102; Joined Cases C-236/08–C-238/08, *Google France SARL v. Louis Vuitton Malletier SA*, 2010 E.C.R. I-2417, ¶ 56.

32. *Google France*, 2010 E.C.R. I-2417, ¶¶ 55–56.

33. *L’Oréal*, 2011 E.C.R. I-6011, ¶ 102.

be taken for granted that they are not. However, both search engines and auction platforms may still be found liable as secondary (contributory) infringers. Furthermore, the court's ruling leaves open the possibility of finding other direct violations. For instance, if a search engine fails to clearly tag the sponsored links in a manner that enables users to recognize them as commercial advertisements, this failure would clash with the requirements set out in Article 6(a) of the E-Commerce Directive and thus result in primary liability.³⁴ Direct liability may also result from negligence for failure to carry out specific legally required duties—such as storing and providing correct information on the identity of users—set out in national law.³⁵

B. NEUTRALITY AS A CONDITION FOR INVOKING SAFE HARBOR

Irrespective of the legal ground on which claims for primary or secondary infringement are raised, an ISP is safe if it has respected the limits set out in Article 14 of the E-Commerce Directive, i.e., if the ISP has assumed a neutral and passive role, and if it has acted expeditiously upon being notified of the infringement.³⁶ The crucial question, therefore, is to what extent an ISP must refrain from activity of its own in order to be considered neutral. In *L'Oréal*, the CJEU seemed to announce a rather strict standard. It observed that

the mere fact that the operator of an online marketplace stores offers for sale on its server, sets the terms of its service, is remunerated for that service and provides general information to its customers cannot have the effect of denying it the exemptions from liability provided for by [the E-Commerce Directive]. Where, by contrast, the operator has provided assistance which entails, in particular, *optimising the presentation of the offers for sale* in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale.³⁷

The decision leaves many issues open-ended, and has been met with different reactions by Member States. Courts in France seem prone to deny the shelter of Article 14 of the E-Commerce Directive to sites providing any service beyond mere content storage (“hosting providers 1.0”).³⁸ In Germany, however, the dominant view is that assistance, such as the presentation of offers on an auction site, is not

34. E-Commerce Directive, *supra* note 3, at 11. (“In addition to other information requirements established by Community law, Member States shall ensure that commercial communications which are part of, or constitute, an information society service comply at least with the following conditions: (a) the commercial communication shall be clearly identifiable as such . . .”).

35. Such a duty exists, for example, in France; negligence of that duty formed one of the claims in the *Tiscali* case. Cour de cassation [Cass.] [supreme court for judicial matters] 1e civ., Jan. 14, 2010, Bull. Civ. I, No. 8 (Fr.). See also *Matulionyte & Nérisson*, *supra* note 9.

36. E-Commerce Directive, *supra* note 3, art. 14.

37. *L'Oréal*, 2011 E.C.R. I-6011, ¶¶ 115–16 (emphasis added).

38. See *Matulionyte & Nérisson*, *supra* note 9, at 61.

detrimental to the ISP's safe harbor if such assistance is rendered in an automated form; if the assistance merely consists of suggestions proffered by operation of algorithms, there is no basis for concluding that the ISP will obtain positive knowledge of, and acquire control over, data relating to the products on sale.³⁹

IV. THE CONCEPT OF *STÖRERHAFTUNG*

As noted above, notwithstanding differences of national law regarding details and terminology, many legal systems embrace the rule that a person assisting a tortfeasor, or inciting him to commit an unlawful act, will be held liable for contributing to the tort. Such liability, however, traditionally requires that the contributor is positively aware of the act resulting in primary infringement, and of the person committing it. In Germany, for example, when an ISP has no actual knowledge of individual persons using its services and is unaware of their conduct, then secondary infringement in the strict sense of aiding and abetting is usually out of question.⁴⁰ Instead, liability is based on the concept of *Störerhaftung*. This concept is derived by analogy from a provision in the civil code entitling proprietors to request that interferences resulting in detrimental effects on their property be removed and enjoined in the future.⁴¹ Objective liability standards apply, and guilt or negligence need not be established.⁴² Showing of detrimental effects is sufficient unless the interference must be tolerated by the proprietor for specific reasons.⁴³

Application of the *Störer* principles in the IP context was well established before the advent of the Internet. Based on those rules, injunctions could be issued, for example, against persons unwittingly storing or transporting infringing goods.⁴⁴ Claims were granted under the following conditions: (1) the defendant is not liable for primary or secondary infringement; (2) an adequate causal link exists between the acts or omissions of the defendant and an (ongoing) infringement of an IP right (resulting in the "interference") and (3) the defendant is (factually and legally) able to remove the cause of the ongoing infringement.⁴⁵

In order to contain the obligations imposed on the defendant, German courts

39. See, e.g., Gerald Spindler, *Europarechtliche Rahmenbedingungen der Störerhaftung im Internet: Rechtsfortbildung durch den EuGH in Sachen L'Oréal/eBay*, 14 MULTIMEDIA UND RECHT [MMR] 703, 705 (2011) (Ger.).

40. Whether the ISP can be held liable for aiding and abetting is a question that is regularly examined (and denied) in cases applying the concept of *Störerhaftung*. See, e.g., Bundesgerichtshof [BGH] [Federal Court of Justice] Mar. 11, 2004, 36 INT'L REV. OF INTELL. PROP. & COMPETITION L. 573, 578, 2005 (Ger.) (*Internet Auction I*).

41. BÜRGERLICHES GESETZBUCH [BGB] [CIVIL CODE], Jan. 2, 2002, BUNDESGESETZBLATT [BGB] I page 42, as amended, § 1004 (Ger.).

42. *Id.*

43. *Id.*

44. See, e.g., Bundesgerichtshof [BGH] [Federal Court of Justice] Jan. 15, 1957, GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT [GRUR] 352, 1957 (Ger.).

45. See, e.g., Bundesgerichtshof [BGH] [Federal Court of Justice] July 12, 2012, GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT [GRUR] 370, ¶ 19, 2013 (Ger.) (*Alone in the Dark*).

have further held that no liability will attach unless the defendant has incurred and neglected certain monitoring duties.⁴⁶ The existence, scope and content of such duties have therefore become the focal point of legal discussions and case law.

Quite importantly, *Störerhaftung* does not provide a basis for damage claims or other sanctions beyond removal of the actual interference and further prevention of the same.⁴⁷ This follows from the fact that the interferer is not liable for primary or secondary infringement according to general tort rules.⁴⁸ Furthermore, the defendant's business is basically innocuous, and the burden of removing infringements committed by others must be weighed against the disruption of the defendant's business that such a duty would cause. On the other hand, this means that the nature of the services rendered should be considered in determining the scope of duties incurred: if the service tends to encourage illicit behavior, the balancing test weighing the interests of the rights holder against those of the ISP may be tipped in favor of the former.⁴⁹

Because *Störerhaftung* only allows rights holders to seek injunctions,⁵⁰ German courts feel free to apply the rule whether or not the activities of the ISP are covered by the safe harbor provisions in the E-Commerce Directive (as implemented in the German Telemedia Act).⁵¹ As expressed by Joachim Bornkamm, the presiding judge of the First Civil Senate of the Federal Court of Justice, "The Court consider[s] [the safe harbor principle] to apply fully to criminal liability and liability for damages, but not injunctive relief."⁵² The court considered that interpretation to be "*acte clair*" (beyond doubt) and therefore did not refer the issue to the CJEU.⁵³

46. Whereas jurisprudence sticks to the term "monitoring duties" (German: *Prüfpflichten*), the literature emphasizes that those duties are of a more comprehensive nature, amounting to a duty to prevent further infringements (not to be confused with negligence of duties of care that result in a stand-alone tort and direct liability for ISPs). See Matthias Leistner, *Störerhaftung und mittelbare Schutzrechtsverletzung*, Supplement to GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT [GRUR] 1, 2010 (Ger.); see also Leistner, *supra* note 9, at 126 (using the phrase "reasonable duty of care to prevent direct infringement"). Although Leistner's observation is certainly correct, this Article will follow the terminology of the jurisprudence by using the phrase "monitoring duties" or its synonyms.

47. See, e.g., Bundesgerichtshof [BGH] [Federal Court of Justice] Jan. 15, 1957, GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT [GRUR] 352, 1957 (Ger.).

48. See *id.*

49. This is illustrated by the RapidShare cases discussed in Part V of this article. See *infra* Part V.

50. See, e.g., Bundesgerichtshof [BGH] [Federal Court of Justice] Jan. 15, 1957, GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT [GRUR] 352, 1957 (Ger.).

51. Telemediengesetz [TMG] [Telemedia Act], Feb. 26, 2007, BUNDESGESETZBLATT [BGB] at 179, 2007 I (Ger.).

52. Joachim Bornkamm, *E-Commerce Directive vs. IP Rights Enforcement: Legal Balance Achieved?*, GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT INT'L 642, 643 (2007). The judge's reasoning appears sound: before the ISP is alerted to an infringement, the ISP is not subject to any obligation. After the ISP is informed, however, Article 14 requires immediate action to remove infringing content. It follows that Articles 12 through 14 do not pose an obstacle for injunctions imposed *after* notification.

53. Leistner, *supra* note 9, at 125. As Leistner states, the argument appears reasonable in light of the preamble to the E-Commerce directive, in particular recital 45:

It remains unclear, however, whether this approach can be reconciled with Article 15 of the E-Commerce Directive, which proscribes any filtering or pre-screening obligations.⁵⁴ Under such circumstances, how can it be found that an ISP has incurred and neglected a duty to monitor? The explanation lies in the distinction between a *general duty* to monitor, which cannot be imposed, and *specific duties* resulting from causes set in the ISP's sphere. This appears compatible with EU law, as expressed in recital 47 of the preamble to the E-Commerce Directive: "Member States are prevented from imposing a monitoring obligation on service providers *only with respect to obligations of a general nature*; this does *not concern monitoring obligations in a specific case* and, in particular, does not affect orders by national authorities in accordance with national legislation."⁵⁵

This principle applies in a clear way when an ISP receives a court order, on the basis of Article 11 of the Enforcement Directive,⁵⁶ to remove infringing content from its Web site. One-time removal of actual content is not sufficient to comply, and recurrence of the same infringement must also be prevented, which necessarily compels some amount of monitoring.⁵⁷ The same reasoning applies when the ISP has been duly notified of an ongoing infringement, without the issue being brought to court.

While the general framework seems to be clear, its details are uncertain. For instance, while the duty to monitor is firmly established once a court order has been received, things are less certain in the pre-trial stage, when rights holders' claims may be exaggerated or even unfounded. How can the ISP tell the difference? Unlike the DMCA,⁵⁸ the E-Commerce Directive lacks specific provisions addressing this problem. As a result, the German Federal Court of Justice has provided guidelines as to when a notification is to be considered serious and plausible enough to give rise to removal and prevention claims.⁵⁹ However, those

[T]he limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds. Such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it. E-Commerce Directive, *supra* note 3, art. 14, at 13.

54. E-Commerce Directive, *supra* note 3, art. 15, at 13.

55. *Id.* at 6, ¶ 48 (emphasis added). Paragraph 48 continues:

This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.

Id.

56. Council Directive 2004/48/EC, on the Enforcement of Intellectual Property Rights, 2004 O.J. (L 157) 76.

57. See Case C-324/09, L'Oréal SA v. eBay Int'l AG, 2011 E.C.R. I-6011, ¶ 144.

58. See 17 U.S.C. § 512(c)(3) (2012).

59. Notification must be concrete enough that its addressee can detect the infringement without an intensive legal and factual examination. The extent of the examination the operator is expected to make depends on the circumstances of the individual case, especially on the gravity of the reported infringements and on the opportunities the operator has to detect them. If the operator of an Internet

guidelines remain fairly vague and general.⁶⁰

V. CASE LAW

A. GENERAL DEVELOPMENTS

The bases for German jurisprudence on ISP liability were set out in the “Internet auction” cases.⁶¹ The Federal Court of Justice confirmed the rule that when infringing articles are sold on an Internet auction platform, the platform provider is not liable under general tort principles as a primary or secondary infringer as long as he does not have actual and concrete knowledge of the acts committed by others.⁶² Damage claims, therefore, cannot be established against the platform provider. Nevertheless, after having been made aware of the infringement, he can be held liable as an interferer, at which point injunctive relief can be granted and preventive measures ordered.⁶³

The rule was subsequently modified with regard to situations in which the alleged primary tort concerns an act of unfair competition. In such situations, the ISP is held liable for committing an independent tortious act under Section 3, the general clause of the German Unfair Competition Act.⁶⁴ This change takes into account the fact that the ISP’s commercial activities create a relevant risk that others will engage in unfair competition. This gives rise to an independent duty of reasonable care to control and limit such risks, the violation of which itself constitutes an act of unfair competition.⁶⁵ In spite of the obvious parallels existing between that line of argument, on the one hand, and the principles of *Störerhaftung* on the other, the Federal Court of Justice has until now rejected suggestions that negligence could be an independent tortious act in trademark as well as in copyright infringement.⁶⁶ *Störerhaftung* therefore remains an accessory to the

marketplace has legitimate doubts concerning the infringement, he must notify the claimant thereof. See Bundesgerichtshof [BGH] [Federal Court of Justice] Aug. 17, 2011, 44 INT’L REV. INTELL. PROP. & COMPETITION L. 123, 2013 (Ger.) (*Perfume Stick*).

60. See *id.*

61. Bundesgerichtshof [BGH] [Federal Court of Justice] Apr. 30, 2008, GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT [GRUR] 702, 2008 (Ger.) (*Internet Auction III*); Bundesgerichtshof [BGH] [Federal Court of Justice] Apr. 19, 2007, GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT [GRUR] 708, 2007 (Ger.) (*Internet Auction II*); Bundesgerichtshof [BGH] [Federal Court of Justice] Mar. 11, 2004, 36 INT’L REV. OF INTELL. PROP. & COMPETITION L. 573, 2005 (Ger.) (*Internet Auction I*). For an account of *Internet Auction I* in English, see Bornkamm, *supra* note 52. All three cases are extensively related in *L’Oréal SA v. eBay International AG*, [2009] EWHC (Ch) 1094, [455] (Arnold, J.) (Eng.).

62. See Bornkamm, *supra* note 52.

63. See *id.*

64. “Unfair commercial practices shall be illegal if they are suited to tangible impairment of the interests of competitors, consumers or other market participants.” BÜRGERLICHES GESETZBUCH [BGB] [CIVIL CODE], Mar. 3, 2010, DAS BUNDESGESETZBLATT [BGBl] 254, § 3, ¶ 2 (Ger.), translation available at http://www.gesetze-im-internet.de/englisch_uwg/englisch_uwg.html#UWGengl_000P3.

65. Bundesgerichtshof [BGH] [Federal Court of Justice] Jul. 12, 2007, GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT [GRUR] 890, 2007 (Ger.) (*Jugendgefährdende Medien bei eBay*).

66. See Leistner, *supra* note 9, at 127. The distinction was somewhat blurred by a decision

main IP infringement, with the consequence, *inter alia*, that counterfeits offered for sale on auction Web sites do not have to be removed by the ISP if the seller was acting privately, and thus did not use the mark “in the course of trade.”⁶⁷

Of particular importance in all those cases are the scope and contents of the preventive duties imposed: What content do they cover? Which preventative measures are required of the ISP? In that regard, it is clear and accepted that, irrespective of the proposition that the safe harbor provisions of the E-Commerce Directive do not apply to injunctive (and preventive) relief under the *Störer* concept, sanctions may not be imposed if they clash with the ban against general filtering obligations in Article 15 of the E-Commerce Directive.⁶⁸ The Federal Court of Justice has therefore emphasized the need to limit the preventive measures imposed to adequate and reasonable filtering that does not jeopardize the defendant’s business model.⁶⁹ Nevertheless, the court has not confined such duties to future identical offers made by the same person, but rather has extended them to infringements that were *essentially of the same character*.⁷⁰ Thus, in the first “Internet Auction” case, concerning offers of watches as “Rolex-replicas,” it was held that if the offers turned out to be infringing, the auction site needed to scrutinize more closely *any future offers* of Rolex watches on its Web site.⁷¹ Likewise, in a case concerning offers of illicit material (computer games glorifying violence and Nazi-type propaganda), an auction site was ordered to prevent not only further offers of the same material by the same persons, but also offers of similar material by any others.⁷² In neither case did the court specify exactly what those measures should be; each defendant was left to identify the most appropriate

finding the holder of an eBay account directly liable for sales of fake products his wife had offered through his account. The court found liability via a false representative or impersonator, due to the fact that the defendant had not taken measures to conceal his password. Bundesgerichtshof [BGH] [Federal Court of Justice] Mar. 11, 2009, GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT [GRUR] 597, 2009 (Ger.) (*Halzband*). In a subsequent decision concerning similar facts (an unknown third party using unsecured WLAN access data to download protected content), the Federal Court of Justice returned to employing the *Störer* principles, refusing to analogize secure wireless account access data to a shared password for an eBay account. Bundesgerichtshof [BGH] [Federal Court of Justice] May 12, 2010, GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT [GRUR] 633 (634), 2010 (Ger.) (*Sommer unseres Lebens*).

67. The issue played a prominent role in the first and third of the *Internet Auction* cases, *supra* note 61, as well as in *L’Oréal v. eBay*:

When an individual sells a product bearing a trade mark through an online marketplace and the transaction does not take place in the context of a commercial activity, the proprietor of the trade mark cannot rely on his exclusive right If, however, owing to their volume, their frequency or other characteristics, the sales made on such a marketplace go beyond the realms of a private activity, the seller will be acting “in the course of trade” within the meaning of those provisions. Case C-324/09, *L’Oréal SA v. eBay Int’l AG*, 2011 E.C.R. I-6011, ¶ 55.

68. See Bornkamm, *supra* note 52.

69. See, e.g., Bundesgerichtshof [BGH] [Federal Court of Justice] July 12, 2007, GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT [GRUR] 890, 2007 (Ger.) (*Jugendgefährdende Medien bei eBay*).

70. See Bornkamm, *supra* note 52.

71. *Id.*

72. Bundesgerichtshof [BGH] [Federal Court of Justice] July 12, 2007, GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT [GRUR] 890, 2007 (Ger.) (*Jugendgefährdende Medien bei eBay*).

technical means for achieving the envisaged result.

The potential range of obligations resulting from the concept of *Störerhaftung* was further illustrated by two recently decided copyright cases concerning the services of RapidShare—a Swiss-based firm that offers digital storage in the cloud that can be accessed world-wide for content of any kind.⁷³ “Normal” users are not charged for storing services, but users opting for a “premium account”—which comes with more storage space and high-speed service—pay a monthly fee.⁷⁴ RapidShare used to offer “premium points” for uploading content that was attractive to others and thus received a high number of downloads; those points could be used for payment of premium account fees. That model was abandoned in 2010 after RapidShare was targeted for inciting copyright piracy.⁷⁵

It is undisputed that among the content stored on RapidShare are files that are illegally made available to the public; several lawsuits have therefore arisen in a number of countries. One of the cases, brought in Germany, concerned links to a computer game (“Alone in the Dark”) that were available on RapidShare. The links were removed after notification by the rights holder, but RapidShare refused to accept that it had a duty to prevent future access to the same game.⁷⁶ The rights holder instigated proceedings, claiming that RapidShare was obligated to remove and prevent the game from becoming available on its Web site or other Web sites that were indicated in the claim.⁷⁷ The appellate court, OLG Düsseldorf, denied the claim, finding that because RapidShare was not aware of individual infringements, it could not be held liable for aiding and abetting.⁷⁸ Furthermore, the court found no reason to hold that RapidShare had neglected a monitoring duty and was therefore liable as an “interferer.” The services offered by RapidShare were considered to be neutral and useful; therefore, the court reasoned, the business model should not be jeopardized by imposing overly strict duties to watch out for infringing content.⁷⁹

Upon further appeal on points of law, the Federal Court of Justice confirmed the Düsseldorf appellate court’s findings with regard to the neutrality and usefulness of the service, but nevertheless arrived at a different result.⁸⁰ The court decided that preventative measures were required, in addition to the expeditious removal of files, from the time that notification of the infringing content was received: RapidShare could, and should, have installed a word filter to retrieve and delete access to all infringing files currently stored in its system, irrespective of the

73. *Security | Our Offer*, RAPIDSHARE, <https://rapidshare.com/security/products> (last visited Feb. 23, 2014).

74. *Id.*

75. Janko Roettgers, *RapidShare Ready to Launch Download Stores*, GIGAOM (June 28, 2010 8:57 AM), <http://gigaom.com/2010/06/28/rapidshare-ready-to-launch-download-stores>.

76. Bundesgerichtshof [BGH] [Federal Court of Justice] July 12, 2012, GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT [GRUR] 370, 2013 (Ger.) (*Alone in the Dark*).

77. *Id.*

78. *See id.*

79. *See id.*

80. Bundesgerichtshof [BGH] [Federal Court of Justice] July 12, 2012, GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT [GRUR] 370, 2013 (Ger.) (*Alone in the Dark*).

persons uploading them.⁸¹ The court was apparently unconcerned that the method may not be completely efficient, as files are easily concealed if uploaded under a slightly different name. The court also considered it appropriate and acceptable that, in order to distinguish files containing the illegally copied computer game from legal content (e.g., collections of photos) stored under the same name, the links retrieved by an automated search had to be re-examined manually.⁸² Finally, it found that imposing an obligation to search a handful of other Web sites for links to the computer game on RapidShare was not exceedingly onerous, and would not disrupt RapidShare's business model.⁸³

About a year after that decision, the Federal Court of Justice decided RapidShare's duty to monitor in a lawsuit filed by GEMA (the collecting society of composers and songwriters) concerning illegal uploads of 4815 music files.⁸⁴ The appellate court below had acknowledged that RapidShare's business model basically deserved protection against disruption, but nevertheless granted the claim on the grounds that RapidShare created a substantial risk of infringements, thus triggering enhanced duties of monitoring and preventive action.⁸⁵ While recognizing that RapidShare had changed its business model so that uploading of commercially attractive (and therefore often illegal) content was not automatically rewarded by premium points, the court found that users were nevertheless likely to associate the Web site with its previous business practices.⁸⁶ Based on such enhanced monitoring duties, RapidShare was ordered to take any possible measures to disable links, both on its own Web site and elsewhere, to any one of the 4815 music titles specified in the claim, irrespective of who provided or linked the file.⁸⁷

The Federal Court of Justice agreed.⁸⁸ The fact that the service had been explicitly recognized as neutral the prior year was explained by the different factual findings of the Düsseldorf court, on which the Federal Court of Justice had relied in its first RapidShare decision.⁸⁹ The court gave little weight to the defendant's argument that because uploading files does not necessarily mean that the copy is illegal or that it will be used for illegal purposes, by deleting such files, legal copies stored for private use could also be destroyed.⁹⁰ The Federal Court of Justice also approved the fact that the appellate court's judgment amounted to a comprehensive market observation duty in regard to all 4815 music files, without limiting it to links which make available an identical copy of the file indicated by

81. *Id.*

82. *Id.*

83. *Id.*

84. Bundesgerichtshof [BGH] [Federal Court of Justice] Aug. 15, 2013, GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT [GRUR] 1030, 2013 (Ger.) (*File-Hosting-Dienst*).

85. *Id.*

86. *Id.*

87. *Id.*

88. Bundesgerichtshof [BGH] [Federal Court of Justice] Aug. 15, 2013, GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT [GRUR] 1030, 2013 (Ger.) (*File-Hosting-Dienst*).

89. *See id.*

90. *Id.*

the complaint.⁹¹ As the court stated, the defendant was “obliged to investigate, through search engines such as Google, Facebook or Twitter using appropriately formulated searches and possibly also with the assistance of so-called web crawlers, whether indications can be found as to further illegal links to its service with regard to the relevant works.”⁹²

VI. CONSEQUENCES FOR TRADEMARK LAW

The German RapidShare cases are remarkable. As noted above, the preventive measures imposed as a consequence of previous conduct were always meant to cover not only *identical* infringements committed by the same person, but also violations of the law that were essentially the same.⁹³ Nevertheless, the second RapidShare decision in particular marks a conspicuous extension of an ISP’s monitoring duties. The logical consequence of the August 2013 decision is that, any time rights holders notify an ISP of infringing content using storage space offered by a cloud operator, the ISP must act not only with regard to the actual copy, but also with regard to all other content possibly stored by the same or other persons; they must undertake a comprehensive and long-term monitoring of any copy reloaded or any link appearing to its service on other Web sites, with no clear guidance from the court as to how this shall be effected. It is easily imagined how the “specific” duties thus incurred in individual cases will accumulate until the line between specific duties and a quasi-general duty to monitor becomes blurred.

Here, we must keep in mind that national systems’ freedom to apply and develop their own doctrines is not limitless. The consequences of German jurisprudence must be measured against mandatory principles of EU law, in the E-Commerce Directive and other legal instruments, including the Charter of Fundamental Rights. In a pending case concerning the unspecified duty of an ISP to block access to a Web site notorious for its infringing content (kino.to), Advocate General Cruz Villalón has declared that while rights holders may require, and courts may order, an ISP to block access to Web sites, it is incompatible with EU law to impose broad, unspecified blocking duties and leaving it to the defendant to figure out ways to cope with them.⁹⁴ If that opinion is endorsed by the CJEU, it might cast a shadow over the recent RapidShare decisions.

But what is the relevance for trademark law? True, the legal provisions and principles apply uniformly to trademark and copyright infringements. However, as mentioned earlier, certain factual divergences between typical copyright and trademark cases may mandate different treatment. Auction platforms are usually less likely to be geared towards encouraging mass infringement, and the role of

91. *Id.*

92. *Id.*

93. See Bundesgerichtshof [BGH] [Federal Court of Justice] July 12, 2007, GEWERBLICHER RECHTSSCHUTZ UND URHEBERRECHT [GRUR] 890, 2007 (Ger.) (*Jugendgefährdende Medien bei eBay*).

94. Case C-314/12, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, 2013, ¶ 77, CURIA (Nov. 26, 2013), <http://curia.europa.eu/juris/celex.jsf?celex=62012CC0314&lang1=en&type=NOT&ancre=>.

ISPs is less “dangerous” in the trademark context because trademarked goods cannot be immediately downloaded. Yet this distinction will not grant immunity against far-reaching duties to monitor: RapidShare, for example, was not simply a rogue Web site, yet some of its features (e.g., acceptance of de-personalized use and payment schemes) were particularly risky and thus justified the imposition of enhanced market observation duties. It is true that the problem of illegal files becoming viral and creating an infinite stream of unauthorized copies has no parallel in trademark law. Still, once a source for counterfeit goods is displayed on the Internet, it may “live on” on other Web sites, even after the original link is removed. While courts may be more cautious to impose extensive monitoring duties in trademark law, given that the technical difficulties of compliance would likely be thornier than in copyright, these duties are not beyond the logic of earlier German jurisprudence.⁹⁵ From the perspective of ISPs, the only positive element of this scenario is that they will not be liable for payment of damages unless their duties are willfully neglected.

How does the story end for RapidShare? Reportedly, RapidShare’s efforts to remove features incentivizing illegal uploads resulted in a mass exodus of users, which could signal the end of its business activities.⁹⁶ It is not clear whether that is good for rights holders; other sites offering similar services are still mushrooming. It is also unclear whether it is wise, as a policy matter, to subject providers of world-wide services to a medley of obligations and sanctions based on many different legal regimes, as happened in RapidShare’s case. Would it be a better and safer solution to provide uniform law, so that the provider can predict legal requirements and adapt its business model accordingly? This is an issue to be addressed in another Article.⁹⁷

95. See discussion *supra*, Part V.A., regarding the Federal Court of Justice’s *Internet Auction I* decision and the accompanying order to monitor for future infringing offers of Rolex watches.

96. Enigmax, *RapidShare: Traffic and Piracy Dipped After New Business Model Kicked In*, TORRENTFREAK (Jan. 9, 2013), <http://torrentfreak.com/rapidshare-traffic-and-piracy-dipped-after-new-business-model-kicked-in-130109>.

97. Edouard Treppoz, *International Choice of Law in Trademark Disputes: From a Territorial Approach to a Global Approach*, 37 COLUM. J.L. & ARTS 557 (2014).