Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 13

Website Blocking Injunctions under EU and U.S. Copyright Law—Slow Death of the Global Internet or Emergence of the Rule of National Copyright Law?

Lukas Feiler

2012

TTLF Working Papers

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

Sponsors

This project was co-sponsored by the Stanford-Vienna Transatlantic Technology Law Forum (Stanford Law School/University of Vienna School of Law), the Stanford Center for E-Commerce, and the Europe Center at the Freeman Spogli Institute for International Studies at Stanford University.

About the Author

Lukas Feiler is an associate at Wolf Theiss Attorneys at Law, Vienna. He earned his law degree from the University of Vienna School of Law in 2008 and a Systems Security Certified Practitioner (SSCP) certification from (ISC)² in 2009. He also studied U.S. cyberspace law and intellectual property law at Santa Clara University. Previous activities include a position of Vice Director at the European Center for E-Commerce and Internet Law, Vienna (2005-2011), a traineeship with the European Commission, DG Information Society & Media, Unit A.3 "Internet; Network and Information Security" in Brussels (2009), software developer positions with software companies in Vienna, Leeds, and New York (2000-2011), and a teaching position for TCP/IP networking and web application development at the SAE Institute Vienna (2002-2006). He is the author of "Information Security Law in the EU and the U.S." (Springer 2011), the co-author of three other books as well as the author of numerous law review articles published *inter alia* in the Santa Clara Computer & High Technology Law Journal, the European Journal of Law and Technology, the Journal of Internet Law, and the Computer Law Review International. He has been a TTLF Fellow since August 2009 and a Europe Center Research Affiliate since November 2009.

General Note about the Content

The opinions expressed in this paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum or any of its partner institutions, or the sponsors of this research project

Suggested Citation

This TTLF Working Paper should be cited as:
Lukas Feiler, Website Blocking Injunctions under EU and U.S. Copyright Law—Slow Death of the Global Internet or Emergence of the Rule of National Copyright Law?, TTLF Working Paper No. 13, http://www.law.stanford.edu/program/centers/ttlf/papers/feiler_wp13.pdf.

Copyright

Abstract

The vast majority of today's online copyright infringements is not anymore committed over peer-to-peer networks but by users accessing regular websites that illegally offer movies, music, or e-books for download (or as a stream). In particular in the EU, right holders are therefore increasingly using a new remedy against online copyright infringement: website blocking injunctions. Obtaining such injunctions, right holders have forced many Internet access providers in the EU to block access to specific infringing websites. This paper analyzes and compares the statutory basis as well as the case law in the EU and the U.S. regarding website blocking injunctions under copyright law against Internet access providers and Internet backbone operators. In particular, the paper examines how the two legal regimes take into consideration the issues of proportionality, the burden on the service providers having to implement the blocking mechanisms, and the interference with the fundamental right to freedom of expression. Moreover, the paper will assess the potential effects of website blocking injunctions. They may lead to a fragmentation of the Internet and thereby also to a fragmentation of markets. On the other hand, website blocking injunctions may be an effective means of enforcing existing copyright laws, thereby strengthening the rule of applicable national law.

Contents

1. Introduction

Copyright infringement by Internet users is a mass phenomenon. It used to be that users mostly obtained infringing copies of musical works, motion pictures, and e-books by using peer-to-peer (P2P) file sharing software. This has lead copyright holders to pursue a two-fold strategy:

First, the distributors of P2P sharing software were, most successfully in the U.S., sued for contributory and/or vicarious copyright infringement as in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster*,[1] *A&M Records, Inc. v. Napster, Inc.*,[2] and *In re Aimster Copyright Litigation.*[3]

Second, claims of direct copyright infringement were brought against many individual users. This was possible because individual users of a P2P network can be easily identified: By participating in a P2P network, users necessarily disclose their IP address to other users of the network. That way, copyright holders—or specialized rights enforcement agencies working on their behalf—were able to obtain the users' IP addresses by joining the P2P network. The actual identity of the users in question could then be uncovered by making a request pursuant to Copyright Act § 512(h) or article 8 of Parliament and Council Directive 2004/48[4]

[1] Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

[2] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

[3] In re Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003).

[4] 2004 O.J. (L 157) 45 (EC).

(hereinafter *Intellectual Property Rights Enforcement Directive* or *IPRED*),[5] respectively, to the users' Internet access providers.

Due to the success of this two-fold enforcement strategy, a new method of distributing infringing content online has become prevalent: Users wishing to download infringing content visit certain websites[6] that provide download-links to files that have been uploaded to file hosting providers (e.g. rapidshare.com, fileserve.com, or hotfile.com).[7] What is most significant from a copyright holder's perspective is that, in this scenario, users do not share their IP address with anyone other than the website providing the download links and the file hosting provider. Different from P2P networks, it is technically impossible for a third party to see who is downloading what.[8]

Facing this new reality, copyright holders have to adopt a new enforcement strategy. Suing the service providers who make the download links available is often not an option since they are located in jurisdictions with weak or non-existing copyright laws. File hosting providers, on the other hand, can claim immunity under the safe

[5] Note however, that IPRED art. 8 does not require Member States to lay down an obligation to reveal subscribers' identities in the context of civil proceedings. *See* Case C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 2008 E.C.R. I-00271, § 58. On the other hand, EU law also does not prohibit Member States from laying down any such obligations. *See* Case C-557/07, LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v. Tele2 Telecommunication GmbH, 2009 E.C.R. I-01227, § 29.

[6] A great number of such sites can be easily identified by using one's favorite search engine to search for the title of any recent blockbuster movie in combination with the term "DVDRip" and the name of any of the file hosting providers referred to in the text.

[7] *See* Janko Roettgers, *Piracy Beyond P2P: One-Click Hosters*, GIGAOM, June 17, 2007, http://gigaom.com/video/one-click-hosters/.

[8] Even a user's Internet access provider could not obtain this information if the communication between the user and the website is encrypted, e.g. by using Hypertext Transfer Protocol Secure (HTTPS).

harbors of Copyright Act § 512(c) and article 14 of Council Directive 2000/31[9] (hereinafter *E-Commerce Directive*) for as long as they have not been notified of a particular infringing file or, in the case they receive such a notification, act expeditiously to remove, or disable access to, the file.[10] Copyright holders therefore have to consistently scan websites known to provide download links in order to notify the infringing files to the corresponding file hosting provider. Since this is a Sisyphean task, copyright holders have, in particular in the EU, increasingly employed a new strategy: seeking injunctions against local Internet access providers and Internet backbone operators, ordering them to block access to websites providing infringing download links.

In the U.S., website blocking injunctions have recently become a hotly debated political issue. The Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011[11] (known as *Protect IP Act* or *PIPA*) was introduced in the U.S. Senate in May 2011 but later put on hold.[12] The Stop Online

[9] 2000 O.J. (L 178) 1 (EC).

[10] The operator of megaupload.com allegedly failed to comply with take-down notices and is thus being prosecuted for copyright infringement. *See* Press Release, U.S. Department of Justice, Justice Department Charges Leaders of Megaupload with Widespread Online Copyright Infringement (Jan. 19, 2012), *available at* http://www.fbi.gov/news/pressrel/press-releases/justice-department-charges-leaders-of-megaupload-with-widespread-online-copyright-infringement.

[11] S. 968, 112th Cong. (2011). The PROTECT IP Act is based on the Combating Online Infringement and Counterfeits Act (COICA), S. 3804, 111th Cong. (2010), which was introduced but not voted on by the full Senate in Congress's previous session. *See* G. Trenton Hooper & Janna M. Wittenberg, *Counterfeiting and the Myth of the Victimless Crime*, 4 LANDSLIDE 41, 45 (2011). *Cf. also* Lavonne D. Burke, *The United States Takes Center Stage in the International Fight Against Online Piracy & Counterfeiting*, 33 HOUS. J. INT'L L. 227 (2010); Ashley S. Pawlisz, *The Bill of Unintended Consequences: The Combating Online Infringement and Counterfeit Act*, 21 DEPAUL J. ART, TECH. & INTELL. PROP. L. 283 (2011).

[12] PIPA was put on hold by Senator Ron Wyden (D-OR) stating that the collateral damage of PIPA would be "speech, innovation and the very integrity of the Internet." Press Release, U.S. Senator

Piracy Act (SOPA) was introduced in the U.S. House of Representatives in October 2011, a markup hearing having been postponed until sometime after Congress returns from its winter recess.[13] Both bills contain provisions that would allow the Attorney General to apply for blocking injunctions, forcing service providers to block "foreign infringing websites." A fierce political debate with still unknown results ensued, disregarding almost completely the already existing possibility to obtain website blocking injunctions under § 512(j)(1)(B)(ii) of the Copyright Act.[14]

In a related development, the U.S. Immigration and Customs Enforcement (ICE) has, since June 2010, used its powers under 18 U.S.C. § 2323 to seize 352 domains,[15] *inter alia* for copyright infringement.[16] However, this power is limited to domains that use top-level domains of registries located in the U.S. (e.g. ".com,"

Ron Wyden, Wyden Places Hold on PROTECT IP Act (May 26, 2011), *available at* http://wyden.senate.gov/newsroom/press/release/?id=33a39533-1b25-437b-ad1d-9039b44cde92.

[13] *See* Hayley Tsukayama, *SOPA Online Piracy Bill Markup Postponed*, POST TECH, Dec. 20, 2011, http://www.washingtonpost.com/blogs/post-tech/post/sopa-online-piracy-bill-markup-postponed/2011/12/20/gIQA6s7a7O_blog.html.

[14] *See Hearing on H.R. 3261, the "Stop Online Privacy Act" Before the House Comm. on the Judiciary,* 112th Cong. (2011) (statement of Maria A. Pallante, Register of Copyrights), *available at* http://www.copyright.gov/docs/regstat111611.html (only stating that "[t]he injunctive relief permitted by SOPA is within the scope of the limitations in section 512(j)").

[15] *See* Press Release, U.S. Immigration and Customs Enforcement, Operation In Our Sites protects American online shoppers, cracks down on counterfeiters (Nov. 28, 2011), *available at* http://www.ice.gov/news/releases/1111/111128washingtondc.htm.

[16] *See* Press Release, U.S. Immigration and Customs Enforcement, "Operation In Our Sites" targets Internet movie pirates (June 30, 2010), *available at* http://www.ice.gov/news/releases/1006/100630losangeles.htm.

".net," and ".org").[17] Thus, domain name seizures by the ICE are no substitute for blocking injunctions as regards foreign websites.

The long-term effects of website blocking injunctions are a contentious issue. On the one hand, they may constitute a significant step away from a global Internet without borders to a more fragmented Internet consisting of many different national "Internets." On the other hand, website blocking injunctions are often the only way in which national laws can be enforced with respect to foreign websites. From this perspective, website blocking injunctions are an effective means of strengthening the rule of applicable national copyright law.

After a short description of the technological background in Part 2, Part 3 will discuss the general limitations of liability for Internet access providers and Internet backbone operators. Part 4 will then examine the possibility of obtaining website blocking injunctions against said providers under EU and U.S. copyright law. In close connection with Part 4, Part 5 will provide a comparative assessment of EU and U.S. copyright law with regard to website blocking injunctions. Part 6 will then elaborate on the potential economic effects of permitting such injunctions and will discuss how they relate to the rule of national copyright law. Finally, Part 7 will provide a concluding summary.

2. Technological Background

Website blocking injunctions can be implemented in one of three ways, each bringing with it a different level of technical complexity, effectiveness, and associated costs:

[17] Cf. Ann Chaitovitz et al., Responding to Online Piracy: Mapping the Legal and Policy Boundaries, 20 COMMLAW CONSPECTUS 1, 4 (2011).

The first and most straightforward method is *DNS blocking*. The Domain Name System (DNS) allows, *inter alia*, the translation of a domain name (e.g. movies.example.com) into the corresponding IP address needed to communicate with any server using the Internet Protocol (IP).[18] To facilitate their customers' use of DNS, Internet access providers typically operate DNS servers which their customers then use to resolve the domain names of all websites they wish to access. An Internet access provider can therefore block an entire domain by making small configuration changes at its DNS server.[19] As regards the effectiveness of this blocking method, it should be noted that the website operator can only circumvent it by using another domain name. The Internet access provider's customers, on the other hand, can perform a circumvention rather easily by configuring their computers to use alternative DNS servers.[20] It should also be stressed that DNS blocking is a method that is unavailable to Internet backbone operators since they do not operate any DNS servers that would be queried by regular users.

The second method is *IP blocking*. Every data packet that is routed over the Internet carries an IP source address and an IP destination address.[21] By blocking data packets with a certain destination address, all direct traffic to a particular IP address can be shut down. Such blocking can be implemented most efficiently by so-called

[18] A short introduction to DNS is provided by CRICKET LIU & PAUL ALBITZ, DNS AND BIND 4 et seq. (5th ed. 2006).

[19] *Cf., e.g.*, Guy Bruneau, *Easy DNS BIND Sinkhole Setup*, SANS INTERNET STORM CENTER, Sept. 9, 2010, http://isc.sans.edu/diary.html?storyid=7930; CRICKET LIU & PAUL ALBITZ, DNS AND BIND 54 et seq. (5th ed. 2006)

[20] *Cf.* Landgericht [LG] [Regional Court] Hamburg, Nov. 12, 2008, docket No. 308 O 548/08 (F.R.G.) (noting that it was possible for the court, "within a few minutes" to find instructions on the Internet for how to perform such a circumvention).

[21] *See* W. Richard Stevens, TCP/IP Illustrated, Volume 1: The Protocols 34 (1994).

black-hole routing. The networks of Internet access providers and backbone operators consist of a large number of routers which maintain so-called routing tables in order to know where to route IP packets destined for a particular IP address.

Black-hole routing refers to the practice of creating an entry in these routing tables that tells the routers to route all IP packets with a particular destination address to the pseudo-interface "Null0" which is equivalent to discarding the packets.[22] Since the routers at the edge of the network (so-called “edge routers”) of an Internet access provider or backbone operator already use the Interior Border Gateway Protocol (iBGP)[23] to synchronize their routing tables, "black hole"-routing information can be distributed very efficiently to all relevant routers using iBGP.[24] To make the edge routers capable of black-hole routing, a simple one-time configuration change has to be made to all of them.[25] Once that has been done, the re-configuration of a single "trigger router" is all that is needed to distribute the

[22] *See* Barry Raveendran Greene & Philip Smith, Cisco ISP Essentials: A Comprehensive Guide to the Best Common Practices for Internet Service Providers 189 et seq. (2002).

[23] The Border Gateway Protocol (BGP) is referred to as iBGP when used within the same provider network (referred to as an "autonomous system"). BGP is specified in Y. REKHTER ET AL., A BORDER GATEWAY PROTOCOL 4 (BGP-4), RFC 4271 (2006), ftp://ftp.rfc-editor.org/in-notes/rfc4271.txt. *Cf.* RAVI MALHOTRA, IP ROUTING 157 (2002).

[24] *See* Barry Raveendran Greene, Remote Triggering Black Hole Filtering—ISP Essentials Supplement 3 (2002), ftp://ftp-eng.cisco.com/cons/isp/essentials/Remote%20Triggered%20Black%20Hole%20Filtering-02.pdf; W. Kumari & D. McPherson, Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF), RFC 5635, at 3 et seq. (2009), http://www.rfc-editor.org/rfc/rfc5635.txt.

[25] This configuration change can be performed by manually issuing a single command on every relevant router. *See* BARRY RAVEENDRAN GREENE, REMOTE TRIGGERING BLACK HOLE FILTERING—ISP ESSENTIALS SUPPLEMENT 6 (2002), ftp://ftp-eng.cisco.com/cons/isp/essentials/Remote%20Triggered%20Black%20Hole%20Filtering-02.pdf.

black-hole routing information to all relevant routers.[26] Thus, to perform subsequent IP blockings, only the trigger router's configuration has to be changed. This technique supports thousands of black-holed IP addresses (or IP address ranges)[27] without any significant impact on the performance of the routers.[28]

Since the list of the IP addresses to be blocked can be centrally maintained at the "triggering router,"[29] the costs of IP blocking are equally low as with DNS blocking once the necessary one-time configuration changes on the edge routers have been performed. However, since these configuration changes on the edge routers are trivial,[30] the cost difference between the first and any subsequent IP blockings is negligible. Furthermore, many diligent Internet access providers and backbone operators have, in fact, already implemented black-hole routing capabilities for security reasons or to fight spam.[31] Thus, IP blocking is generally not more expensive than DNS blocking.

However, IP blocking has also the significant disadvantage of a very high risk of over-blocking. A single IP address is often used to host multiple websites, and

---

[26] See id. at 7.

[27] See id. at 8.

[28] *See id.* at 2 (noting that black-hole routing, if performed on routers that are equipped with application-specific integrated circuits (ASICs), "has zero impact in the performance of the router").

[29] *See id.* at 10 (noting that remote-triggered black-hole routing "helps minimize the operational overhead by having one router in one location holding the master list (i.e. the trigger router)").

[30] *See supra* note 25.

[31] *Cf., e.g.,* European Network & Information Security Agency [ENISA], Provider Security Measures Part 1: Security and Anti-Spam Measures of Electronic Communication Service Providers Survey 4 (2006), *available at* http://www.enisa.europa.eu/act/res/other-areas/anti-spam-measures/studies/provider-security-measures-1/at_download/fullReport (stating that 41% of service providers in the EU implemened "Blackholing/Sinkholing").

indeed often hundreds of them.[32] Thus, when IP blocking is used, the blocking of one website will often automatically result in the blocking of numerous other (typically unrelated) websites. Significantly, it is typically not possible for anyone other than the hosting provider hosting the websites in question to determine with certainty whether an IP address is used by multiple websites, let alone how many of them.[33] The extent of over-blocking can therefore typically not be determined with certainty from an *ex ante* perspective.

IP blocking can also be circumvented rather easily by a website operator by obtaining a new IP address and re-configuring its domain name so that it resolves to that new IP address. Users, on the other hand, can only circumvent IP blocking by relaying their traffic over a server that (1) is connected to a different Internet access provider and (2) if the blocking is implemented at the backbone-level, routes its traffic over a different Internet backbone operator and is therefore not affected by the blocking measure. The relaying of traffic is, however, likely to significantly increase the latency and reduce the user's bandwidth which may make the website in question unusable.

The third method is *URL blocking*. This form of blocking requires that the service provider not only examines the so-called headers of IP packets (containing the source and destination IP address) but also the contents of IP packets. This can be

[32] *Cf.* Steven J. Murdoch & Ross Anderson, *Tools and Technology of Internet Filtering, in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 57, 66 (2008) (citing Ben Edelman, Web Sites Sharing IP Addresses: Prevalence and Significance, Berkman Center for Internet and Society (Sept. 2003), http://cyber.law.harvard.edu/archived_content/people/edelman/ip-sharing).

[33] However, tools exist that reveal at least some of the domains sharing an IP address. *See, e.g.*, http://www.domaintools.com/research/reverse-ip (last accessed Feb. 16, 2012).

done either by so-called deep packet inspection to be performed by the service provider's routers or by implementing a proxy all users are forced to use to access the web. Irrespective of the method of implementation, such URL blocking is not only counter to the Internet's architectural principles[34] but also highly resource-intensive and therefore costly.[35] Indeed, for an Internet access provider to perform URL blocking, it would have to make very substantial investments into its infrastructure.[36] For Internet backbone operators, URL blocking would be even more costly.[37] Ultimately, both types of service providers would have to significantly restructure their networks to implement this type of website blocking.

As regards its effectiveness, URL blocking combines the advantages of DNS blocking and IP blocking: For website operators, a circumvention would be as difficult as in the case of DNS blocking while for users, it would be as difficult as in the case of IP blocking. URL blocking is also the most precise method which carries the lowest risk of over-blocking. However, as mentioned above, it is also the most costly method.

---

[34] *Cf.* BARBARA VAN SCHEWICK, INTERNET ARCHITECTURE AND INNOVATION 88 et seq. (2010) (discribing the Internet's layering principle that would be disrespected if Internet access providers or Internet backbone operators—which perform services on the link layer and the Internet layer—were to differentiate between traffic based on application layer information such as a URL).

[35] *Cf.* UK OFFICE OF COMMUNICATIONS, "SITE BLOCKING" TO REDUCE ONLINE COPYRIGHT INFRINGEMENT 45 (2011), *available at* http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf.

[36] The existing infrastructure of most Internet access providers is not capable of URL blocking. Thus, new network devices with significant processing capabilities would have to be acquired and integrated into the service provider's network.

[37] Internet backbone providers typically have to handle a very high bandwidth and thus would have to invest in equipment that has even more processing capabilities. Since an outage of such equipment would also affect legitimate sites, solutions with high availability in form of redundant hardware would be needed.

3. Limitations of Internet Access Provider and Backbone Operator Liability

Before discussing the possibility of injunctions under copyright law, the legal frameworks under EU and U.S. law limiting service provider liability are discussed.

3.1 The EU E-Commerce Directive

Parliament and Council Directive 2000/31[38] (hereinafter *E-Commerce Directive*), *inter alia*, harmonizes the issue of liability of providers of "information society services." Such services are defined as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."[39]

In particular, the E-Commerce Directive provides a liability exemption[40] for "mere conduit" services as regards civil as well as criminal liability, including liability under copyright law.[41]

---

[38] 2000 O.J. (L 178) 1 (EC).

[39] E-Commerce Directive art. 2(a) in conjunction with art. 1(2) of Parliament and Council Directive 98/34, 1998 O.J. (L 204) 37 (EC) as amended by Parliament and Council Directive 98/48, 1998 O.J. (L 217) 18, 21 (EC) (further defining "at a distance" as meaning "that the service is provided without the parties being simultaneously present"; "by electronic means" as meaning "that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means"; and "at the individual request of a recipient of services" as meaning "that the service is provided through the transmission of data on individual request"). That the service has to be "normally provided for remuneration" does not require that the remuneration stems from a service recipient. *See* E-Commerce Directive recital 18. *Cf.* Legislative Development, *Scope of the E-Commerce Directive 2000/31/EC of June 8, 2000*, 7 COLUM. J. EUR. L. 473, 475 (2001) (noting that the Directive also covers "services provided free of charge to the recipient, e.g. funded by advertising or sponsorship revenue").

[40] *Cf.* CLAUS KASTBERG NIELSEN ET AL., STUDY ON THE ECONOMIC IMPACT OF THE ELECTRONIC COMMERCE DIRECTIVE 16 et seq. (2007), *available at* http://ec.europa.eu/internal_market/e-

Mere conduit services are defined as information society services that consist of (1) "the transmission in a communication network of information provided by a recipient of the service"; or (2) "the provision of access to a communication network."[42] This covers Internet backbone operators ("transmission *in* a communication network") as well as Internet access providers ("access *to* a communication network").[43]

The E-Commerce Directive stipulates that a provider of a mere conduit service should not be liable for the information transmitted if the provider neither (1) initiates the transmission, nor (2) selects the receiver of the transmission, nor (3) selects or modifies the information contained in the transmission.[44] Internet backbone operators and Internet access providers are therefore shielded from liability even if they have actual knowledge of the information in question and its illegal nature.

However, pursuant to article 12(3) of the E-Commerce Directive, the liability exemption does "not affect the possibility for a court or administrative authority […]

---

commerce/docs/study/ecd/%20final%20report_070907.pdf (discussing the economic significance of the Directive's limited liability provisions in general terms).

[41] For a general discussion of Member State legislation and national court decisions see THIBAULT VERBIEST ET AL., STUDY ON THE LIABILITY OF INTERNET INTERMEDIARIES 32 (2007), *available at* http://ec.europa.eu/internal_market/e-commerce/docs/study/ecd/%20final%20report_070907.pdf.

[42] E-Commerce Directive art. 12(1).

[43] *Cf.* Patrick Van Eecke & Barbara Ooms, *ISP Liability and the E-Commerce Directive: A Growing Trend Toward Greater Responsibility for ISPs*, 11 J. INTERNET L. 3, 4 (2007) (referring to backbone operators and Internet access providers); Pablo Asbo Baistrocchi, *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce*, 19 SANTA CLARA COMPUTER & HIGH TECH. L.J. 111, 119 (2002) (stating that "transmission *in* a communication network" (emphasis added) refers to an ISP "acting as a mere 'carrier' of data provided by third parties through its network").

[44] E-Commerce Directive art. 12(1).

of requiring the service provider to terminate or prevent an infringement."[45] In particular, this includes injunctions that order the "the disabling of access to [illegal information]."[46]

Remarkably, article 12(3) of the E-Commerce Directive does not explicitly require that the injunctions issued pursuant to that provision have a certain level of specificity. However, E-Commerce Directive article 15 states that "Member States shall not impose a general obligation on providers […] to monitor the information which they transmit or store."[47]

[45] E-Commerce Directive art. 12(3).

[46] E-Commerce Directive recital 45.

[47] E-Commerce Directive art. 15(1). Note that Parliament and Council Directive 2002/58, art. 15, 2002 O.J. (L 201) 37, 46 (EC), as amended (hereinafter *ePrivacy Directive*), allows Member States to adopt "legislative measures providing for the retention of data for a limited period" justified on the grounds that they are "necessary, appropriate and proportionate measure[s] within a democratic society to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system." ePrivacy Directive art. 15(1). Parliament and Council Directive 2006/24, 2006 O.J. (L 105) 54 (commonly referred to as the "Data Retention Directive") goes one step further, requiring Member states to introduce obligations for "providers of publicly available electronic communications services or of public communications networks" (these are "mere conduit" providers) "with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime." *Id*. art. 1(1). For an extensive discussion of the Data Retention Directive see Lukas Feiler, *The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection*, 1 EUR. J. OF L. & TECH. 3 (2010), http://ejlt.org//article/view/29/75. However, neither ePrivacy Directive art. 15 nor the Data Retention Directive have direct relevance for the question of when an injunction amounts to a general monitoring obligation prohibited under art. 15 of the E-Commerce Directive.

3.2 The Communications Decency Act and Copyright Act § 512(a)

Section 502 of the Communications Decency Act of 1996[48] (hereinafter *CDA*) which is codified at 47 U.S.C. § 230 and therefore often simply referred to as "section 230" is considered "one of the most important and successful laws of cyberspace."[49] It broadly exempts interactive computer service providers[50] from liability, irrespective of whether the provider had actual knowledge of the information in question.[51]

However, the immunity provided by § 230 does not apply with regard to "any law pertaining to intellectual property."[52] As regards injunctions under copyright law, Internet access providers may therefore only find an exemption of liability within the Copyright Act.

---

[48] Pub. L. No. 104-104, Title V, 110 Stat. 56, 113 (1996).

[49] David Lukmire, Can the Courts Tame the Communications Decency Act?: The Reverberations of Zeran v. America Online, 66 N.Y.U. ANN. SURV. AM. L. 371, 372 (2010) (citing Recent Case, Federal District Court Denies § 230 Immunity to Website That Solicits Illicit Content - FTC v. Accusearch, Inc., 121 HARV. L. REV. 2246, 2253 (2008)). For an empirical study of 184 decisions applying § 230 between its effective date, February 8, 1996, and September 30, 2009 see David S. Ardia, Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act, 43 LOY. L.A. L. REV. 373 (2010).

[50] *See* 47 U.S.C. § 230(f)(2) (defining "[i]nteractive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet […].").

[51] *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 333 et seq. (4th Cir. 1997) (holding that § 230 eliminates publisher liability—which is based on a strict liability standard—as well as distributor liability which is based on liability upon notice (or actual knowledge): "like strict liability, liability upon notice has a chilling effect on the freedom of Internet speech"; further noting that "Congress has indeed spoken directly to the issue by employing the legally significant term 'publisher,' which has traditionally encompassed distributors and original publishers alike").

[52] 47 U.S.C. § 230(e)(2).

Section 512(a) of the Copyright Act provides that a service provider is, under certain conditions, not liable for infringement of copyright by reason of "transmitting, routing, or providing connections for" material through a system or network that is controlled or operated by or for the service provider.[53] This wording—in particular the general reference to "routing"—makes clear that not only Internet access providers but also Internet backbone operators are covered.

To benefit from this liability exemption, the following conditions must be met: (1) the transmission of the material was not initiated by or at the direction of the service provider;[54] (2) the service is provided through an automatic technical process without selection of the material by the service provider;[55] (3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;[56] (4) copies of the material made by the service provider in the course of an intermediate or transient storage are maintained in a manner ordinarily accessible only to anticipated recipients and only for the minimum amount of time;[57] and (5) the material is transmitted through the system or network without modification of its content.[58]

Furthermore, the provider has to (1) adopt, reasonably implement, and inform its subscribers about a policy for the termination of subscribers that are repeat

[53] 17 U.S.C. § 512(a). This liability exemption also covers liability for copyright infringement "by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections." *Id.*

[54] 17 U.S.C. § 512(a)(1).

[55] 17 U.S.C. § 512(a)(2).

[56] 17 U.S.C. § 512(a)(3).

[57] 17 U.S.C. § 512(a)(4).

[58] 17 U.S.C. § 512(a)(5).

infringers[59] and (2) accommodate and not interfere with certain technical measures that are used by copyright owners to identify or protect copyrighted works.[60]

However, pursuant to § 512(a) of the Copyright Act, this limitation of liability does not apply with regard to injunctive or other equitable relief as provided in § 512(j) which will be further discussed below.

4. The Possibility of Obtaining Website Blocking Injunctions under Copyright Law

What is clear from the brief discussion of EU and U.S. law above is that a great difference is made between liability and injunctions. While Internet access providers and Internet backbone operators are generally protected from any liability for damages, E-Commerce Directive article 12 as well as Copyright Act § 512(a) leave open the possibility of injunctive relief. Such injunctive relief is provided by article 8 of Parliament and Council Directive 2001/29[61] (hereinafter *Information Society Directive*) as well as § 512(j) of the Copyright Act.

4.1 Information Society Directive Article 8

Article 8(3) of the Information Society Directive provides that right holders have to be 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."[62]

[59] 17 U.S.C. § 512(i)(1)(A).

[60] 17 U.S.C. § 512(i)(1)(B) in conjunction with § 512(i)(2).

[61] 2001 O.J. (L 167) 10.

[62] Information Society Directive art. 8(3).

The wording of this provision focuses on the infringement by those who make use of the intermediary's services and does not require that the intermediary itself infringes any copyright (or related right). An injunction is available even if the provider's actions are exempt under Information Society Directive article 5(1)(a) and therefore do not constitute copyright infringement.[63] This is because intermediaries such as Internet access providers and Internet backbone operators themselves typically do not commit any copyright infringement by transmitting illegal copies: Information Society Directive article 5(1)(a) provides that temporary acts of reproduction do not constitute copyright infringement if (1) they are transient or incidental; (2) they are an integral and essential part of a technological process; (3) their sole purpose is to enable a transmission in a network between third parties by an intermediary; and (4) they have no independent economic significance.[64]

The scope of a potential injunction under Information Society Directive article 8 has to be determined in light of Parliament and Council Directive 2004/48[65] (hereinafter

[63] Information Society Directive recital 59. Cf. also Commission Staff Working Document: Analysis of the application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights in the Member States, at 16, SEC (2010) 1589 final (Dec. 12, 2010) (stating that "neither Article 11 (third sentence) of [Directive 2004/48], nor Article 8(3) of Directive 2001/29 link injunctions with the liability of an intermediary"). The reason Information Society Directive article 8(3) does not link injunctions with secondary liability is that secondary liability has not been harmonized at the EU level. See Silke von Lewinski & Michel Walter, Information Society Directive, in EUROPEAN COPYRIGHT LAW: A COMMENTARY 921, 1086 (Michel Walter & Silke von Lewinski eds., 2010).

[64] This exception—like any other exception or limitation of copyright—suffers from legal uncertainty caused by the so-called "three-step test" which is set out in Information Society Directive article 5(5): *inter alia* article 5(1)(a) shall only be applied "in certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder."

[65] 2004 O.J. (L 157) 45 (EC).

Intellectual Property Rights Enforcement Directive or *IPRED*).[66] While not directly affecting Information Society Directive article 8,[67] IPRED article 11(3) extended the right to apply for an injunction against intermediaries to all intellectual property rights. Thus, the holding of the European Court of Justice (hereinafter *ECJ*) in *L'Oréal SA v. eBay International AG*[68] with regard to IPRED article 11(3) also has to be applied to Information Society Directive article 8.[69] In that case, the ECJ held that injunctions under IPRED article 11(3) are not limited to "measures which contribute […] to bringing [infringements] to an end" but may also cover measures "which contribute to […] preventing further infringements of that kind."[70]

Thus, in *Scarlet Extended SA v. Société Belge des auteurs, compositeurs et éditeurs (SABAM)*,[71] the ECJ held that Information Society Directive article 8(3) and IPRED article 11 must allow national courts to order ISPs whose services are being used by a third party for infringement "to take measures aimed not only at bringing to an end

[66] *Cf.* Michel Walter & Dominik Goebel, *Enforcement Directive*, *in* EUROPEAN COPYRIGHT LAW: A COMMENTARY 1193, 1218 (Michel Walter & Silke von Lewinski eds., 2010).

[67] *See* IPRED recital 23.

[68] Case C-324/09, L'Oréal SA v. eBay International AG, 2011 E.C.R. I-00000.

[69] *See* Twentieth Century Fox Film Corp. v. British Telecommunications PLC, [2011] EWHC 1981 (Ch.), July 28, 2011, § 156, *available at* http://www.bailii.org/ew/cases/EWHC/Ch/2011/1981.html (U.K.) (relying on *L'Oréal SA v. eBay International AG* for the interpretation of Information Society Directive art. 8(3)).

[70] Case C-324/09, L'Oréal SA v. eBay International AG, 2011 E.C.R. I-00000, § 144. *See also* Case C-70/10, Scarlet Extended SA v. Société Belge des auteurs, compositeurs et éditeurs (SABAM), 2011 E.C.R. I-0000, § 31.

[71] Case C-70/10, Scarlet Extended SA v. Société Belge des auteurs, compositeurs et éditeurs (SABAM), 2011 E.C.R. I-0000.

infringements already committed against intellectual-property rights using their information-society services, but also at preventing further infringements."[72]

The question whether Internet access providers qualify as "intermediaries" has been answered in the affirmative by the ECJ in the case of *LSG v. Tele2*.[73] The Court reasoned that Internet access providers who "merely enable clients to access the Internet, even without offering other services […] provide a service capable of being used by a third party to infringe a copyright or related right."[74]

What has, so far, not been at issue in any reported court case in the EU, is whether Internet backbone operators are to be considered "intermediaries" too. Information Society Directive recital 59—to which the ECJ also referred in *LSG v. Tele2*[75]—states that "rightholders should have the possibility of applying for an injunction against an intermediary who carries a third party's infringement of a protected work or other subject-matter in a network." This wording strongly indicates that the term "intermediary" also covers Internet backbone operators since they "carr[y] [infringements] in a network."

4.1.1 Relation to the E-Commerce Directive

Recital 16 of the Information Society Directive states that "[t]his Directive is without prejudice to provisions relating to liability in [the E-Commerce Directive]." This reference is to be interpreted as a reference to all articles under section 4 of the

[72] *Id.* at § 31.

[73] Case C-557/07, LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v. Tele2 Telecommunication GmbH, 2009 E.C.R. I-01227.

[74] *Id.* at § 43.

[75] *Id.* at § 44.

E-Commerce Directive ("Liability of intermediary service providers"). In particular, this also includes E-Commerce Directive article 15 which, as mentioned *supra* in Part 3.1, prohibits Member States from imposing any "general" monitoring obligations. Thus, injunctions against Internet access providers (and Internet backbone operators) may only be issued pursuant to Information Society Directive article 8 if they do not result in "general" monitoring obligations.[76]

This raises the question: When does an injunction potentially amount to a general monitoring obligation prohibited under the E-Commerce Directive?

In *Scarlet Extended SA v. Société Belge des auteurs, compositeurs et éditeurs (SABAM)*,[77] a case concerning copyright infringement via peer-to-peer networks, the ECJ held that an injunction that requires an Internet access provider to install a filtering system that "would oblige it to actively monitor all the data relating to each of its customers" would amount to general monitoring as prohibited under E-Commerce Directive article 15.[78]

Consequently the ECJ, to determine whether an injunction is of a general nature, does not consider the specificity of the copyrighted works on the basis of which the injunction is sought[79] but only (1) the relative amount of traffic to be monitored for

[76] *Cf.* Case C-324/09, L'Oréal SA v. eBay International AG, 2011 E.C.R. I-00000, § 139; Case C-70/10, Scarlet Extended SA v. Société Belge des auteurs, compositeurs et éditeurs (SABAM), 2011 E.C.R. I-0000, § 35.

[77] Case C-70/10, Scarlet Extended SA v. Société Belge des auteurs, compositeurs et éditeurs (SABAM), 2011 E.C.R. I-0000.

[78] *Id.* at § 40. *Cf. also* Case C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV, 2012 E.C.R. I-0000, § 34 (using the same criteria with regard to a hosting provider).

[79] In *Scarlet Extended SA v. SABAM*, the ECJ noted that the injunction is "intended to protect not only existing works, but also future works that have not yet been created at the time when the

each customer and (2) the relative amount of customers for which monitoring is to be performed.

On this basis, it seems highly unlikely that DNS blocking and IP blocking which both only concern traffic data but not the content of communications[80] would be considered a means of "general" monitoring. URL blocking, on the other hand, requires that the contents of all packets be examined to determine whether they are part of a request to a blocked URL. Thus, due to the prohibition of "general" monitoring obligations pursuant to E-Commerce Directive article 15, URL blocking is significantly more problematic than IP blocking or DNS blocking.

4.1.2 An Overview of Court Cases in the Member States

An increasing number of national court cases have dealt with injunctions against Internet access providers under EU copyright law. The vast majority of court decisions granted an injunction:

In the most recent case of *Constantin Film Verleih GmbH v. UPC Telekabel Wien GmbH*,[81] the Commercial Court Vienna issued an injunction against the Internet

---

[filtering] system is introduced." Case C-70/10, Scarlet Extended SA v. Société Belge des auteurs, compositeurs et éditeurs (SABAM), 2011 E.C.R. I-0000, § 47. However, the Court only considered this fact in connection with the interference with fundamental rights and not with regard to the prohibition on "general" monitoring obligations pursuant to E-Commerce Directive art. 15.

[80] From a technical perspective, DNS blocking—in contrast to IP blocking—does, of course, require the processing of the contents of data packets used to resolve a domain name. However, these data packets are directly addressed to the DNS servers operated by the Internet access provider. Thus, DNS blocking does not require the monitoring of the contents of all traffic but only of that which is addressed to the Internet access provider's DNS servers.

[81] Handelsgericht [HG] Wien, May 13, 2011, docket No. 22 Cg 120/10f (Austria) (unpublished, on file with author), *rev'd*, Oberlandesgericht [OLG] [Superior Regional Court] Wien, Nov. 14, 2011, docket No. 1 R 153/11v (Austria) (unpublished, on file with author).

access provider UPC, ordering it to block access to the website kino.to which made movies available to the public, for which the plaintiff held the rights. In its order, the court required UPC to implement blocking at the DNS-level as well as on the IP-level and gave the plaintiff the right to subsequently specify additional IP addresses to which the blocking should be extended.[82] On appeal, the Superior Court Vienna also sided with the plaintiff but held that an injunction must not specify the means (e.g. DNS blocking or IP blocking) by which the defendant has to comply with its obligation.[83]

In *IFPI Finland v. Elisa Corp.*, the Helsinki District Court held that Elisa, one of Finland's largest Internet access providers,[84] had to block access to The Pirate Bay by (1) removing the domain names used by The Pirate Bay from its DNS servers and (2) blocking traffic to the website's IP addresses.[85]

In *VZW Belgian Anti-Piracy Federation v. NV Telenet*,[86] the Antwerp Court of Appeals issued an injunction against the two largest Internet access providers in Belgium,[87] ordering them to use DNS blocking to prevent their customers from accessing eleven specific domains used to host the website The Pirate Bay.[88] IP

[82] See id. at 3.

[83] Oberlandesgericht [OLG] [Superior Regional Court] Wien, Nov. 14, 2011, docket No. 1 R 153/11v (Austria) (unpublished, on file with author).

[84] According to its website, Elisa serves approximately 2.2 million consumers. *See* http://www.elisa.com/on-elisa/ (last accessed Feb. 15, 2012).

[85] Helsingin käräjäoikeus [Helsinki District Court], Oct. 26, 2011, docket No. H 11/20937 (Finland) (unpublished, on file with author).

[86] Hof van Beroep [Court of Appeal] Antwerpen, Sept. 26, 2011, docket No. 2011/8314 (Belgium), *available at* http://nurpa.be/files/20111004_BAF-Belgacom-Telenet-DNS-blocking.pdf.

[87] NV Telenet ("Telenet") and NV Van Publiek Recht Belgacom ("Belgacom"). *See id.* at 12.

[88] *Id.* at 15-16.

blocking was explicitly rejected by the court due to the higher risk of blocking legitimate information contained on websites hosted on the same IP address as the websites of The Pirate Bay.[89]

In *Twentieth Century Fox Film Corp. v. British Telecommunications PLC*,[90] the British High Court issued an injunction against the Internet access provider British Telecom (hereinafter *BT*), ordering it to block access to the website www.newzbin.com which essentially makes available links to infringing content in exchange for payment and thereby infringes U.K. copyright law.[91] To do so, BT was ordered to use a system referred to as "Cleanfeed" which it already employed to block URLs and IP addresses hosting child pornography.[92] Thus, the court had no trouble concluding that the costs to BT would be modest and the injunction therefore proportional.[93]

In *IFPI Denmark v. Tele2 A/S*,[94] the City Court of Copenhagen ordered the Internet access provider Tele2 to block its subscribers' access to the Russian website AllOfMP3.com which made music files publicly available in Denmark without a

[89] *See id.* at 14.

[90] Twentieth Century Fox Film Corp. v. British Telecommunications PLC, [2011] EWHC 1981 (Ch.), July 28, 2011 (U.K.), *available at* http://www.bailii.org/ew/cases/EWHC/Ch/2011/1981.html.

[91] *See id.* at § 113. This had already been established in a case brought against the previous operators of the website. *See Twentieth Century Fox Film Corp v. Newzbin Ltd.*, [2010] EWHC 608 (Ch.), Mar. 29, 2010 (U.K.), *available at* http://www.bailii.org/ew/cases/EWHC/Ch/2010/608.html.

[92] For a description of "Cleanfeed," see Twentieth Century Fox Film Corp. v. British Telecommunications PLC, [2011] EWHC 1981 (Ch.), July 28, 2011, §§ 70 et seq. (U.K.), *available at* http://www.bailii.org/ew/cases/EWHC/Ch/2011/1981.html.

[93] *See id.* at §§ 177, 200.

[94] Byret [City Court] Copenhagen, Oct. 25, 2006, docket No. F1-15124/2006, *available at* http://www.dr.dk/NR/rdonlyres/EF2AAB7A-0E04-4963-963A-463CD7550D72/361965/tele2_ke.pdf (Denmark).

license to do so.[95] The court ordered Tele2 to take all necessary measures but stated that blocking at DNS-level was both sufficient and would not lead to any noticeable costs.

In *SABAM v. Scarlet SA*,[96] the District Court of Brussels granted an order requiring the Internet access provider Scarlet (previously Tiscali) to block the transfer of all peer-to-peer traffic that infringes the rights administered by the Belgian collecting society SABAM. This judgment was appealed by the defendant to the Brussels Cour d'Appel (Court of Appeal) which referred the question of whether such a broad injunction was permissible under EU law to the ECJ. As discussed *supra* in Part 3.1, the ECJ held that such a broad injunction in particular violated the prohibition on "general" monitoring obligations set out in E-Commerce Directive article 15.

In *Telenor v. IFPI Denmark*,[97] the Danish Supreme Court upheld an injunction against the Internet access provider Telenor (formerly DMT2 A/S also known as Tele2) ordering it to take all necessary measures to prevent access by its customers to the website thepiratebay.org. The Court also stated that blocking at the DNS-level, as chosen by Telenor, was sufficient to comply with the injunction.[98]

---

[95] Cf. Commission Report to the Council, the European Parliament and the Economic and Social Committee on the application of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, at 10, SEC(2007) 1556 (Nov. 30, 2007).

[96] Tribunal de Premiere Instance de Bruxelles [Court of First Instance of Brussels], June 29, 2007, docket No. 04/8975/A, *available at* http://www.juriscom.net/documents/tpibruxelles20070629.pdf. For a translation see SABAM v. S.A. Scarlet, District Court of Brussels, No. 04/8975/A, Decision of 29 June 2007, published in CAELJ Translation Series #001 (Mady, Bourrouilhou, & Hughes, trans.), 25 CARDOZO ARTS & ENT. L.J. 1279 (2008).

[97] Højesterets [Supreme Court], May 27, 2010, docket No. 153/2009, *available at* http://www.domstol.dk/hojesteret/Documents/Domme/153-09.pdf (Denmark).

[98] *Id.* at 5.

In *Bergamo Public Prosecutor's Officer v. Kolmisappi*,[99] the Italian Supreme Court of Cessation upheld an injunction requiring all Internet access providers operating in Italy to block access to www.thepiratebay.org as part of a preventative seizure in criminal proceedings.

The Swedish case of *Columbia Pictures Industries Inc v. Portlane AB*[100] is also often mentioned in this context. A Swedish court of appeals ordered the Internet access providers Portlane AB and Black Internet AB to block access, respectively to tracker.openbittorrent.com and The Pirate Bay. However, this case is not fully comparable to the other cases since both providers directly acted as Internet access providers for the respective website operators.

Similarly, in the German case of *Columbia Pictures Industries Inc. v. CB3ROB Ltd. & Co. KG*,[101] the defendant was enjoined from serving as an Internet access Provider for The Pirate Bay.

Cases in which a court refused to issue a website blocking injunction were reported from Germany, the Netherlands, Norway, and Ireland. Remarkably, none of the cases present persuasive arguments for why injunctions should not be issued against Internet access providers pursuant to Information Society Directive article 8:

---

[99] Cass., sez. III penale, Sept. 29, 2009, n.49437/09 (Italy), *available at* http://blog.quintarelli.it/files/cassazione-sentenza-49437-2009.pdf.

[100] Hovrätt [HovR] [Appeals Court], May 21, 2010, docket No. Ö 7131-09, Ö 8773-09, and Ö 10146-09, May 21, 2010 (Swed.) (unpublished). A press release issued by the court is available at http://www.svea.se/Om-Sveriges-Domstolar/Pressrum/Nyhetsarkiv/2010/Svea-hovratt-meddelar-interimistiska-vitesforbud-avseende-medverkan-till-upphovsrattsintrang-pa-Internet-hovrattens-mal-O-7131-09-O-8773-09-och-O-10146-09/ (last accessed Feb. 16, 2012).

[101] Landgericht [LG] [Regioinal Court] Hamburg, May 6, 2010, docket No. 310 O 154/10 (F.R.G.), *available at* http://torrentfreak.com/static/injunction.zip.

In three cases before German courts, injunctive relief was denied because Information Society Directive article 8(3) has not been fully transposed into German law: In *EMI v. Hansenet*,[102] the Regional Court Cologne argued that no provision of German statutory law would permit an injunction without a finding of secondary liability. Furthermore, it also held that existing German law could not be interpreted in conformity with Information Society Directive article 8(3) since that provision would not say anything about the specific measures to be ordered by a court. In *Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte (GEMA) v. Deutsche Telekom*,[103] the Regional Court Hamburg explicitly stated that the blocking of websites could currently not be enforced since Information Society Directive article 8(3) has not been fully transposed into German law.[104] Lastly, in a case concerning the website G-Stream.in,[105] the Superior Regional Court Hamburg denied injunctive relief and also stated that Information Society Directive article 8(3) would not require Member States to provide for blocking injunctions.

In light of the ECJ's judgment in *Scarlet Extended SA v. Société Belge des auteurs, compositeurs et éditeurs (SABAM)*,[106] German courts will have to reconsider their interpretation of Information Society Directive article 8(3) and the German

[102] Landgericht [LG] [Regional Court] Köln, Aug. 31, 2011, docket No. 28 O 362/10, 2011 Multimedia und Recht [MMR] 833 (F.R.G.).

[103] Landgericht [LG] [Regional Court] Hamburg, Mar. 12, 2010, docket No. 308 O 640/08, 2010 Multimedia und Recht [MMR] 488 (F.R.G.).

[104] *Id.* at 490.

[105] Oberlandesgericht [OLG] [Superior Regional Court] Hamburg, Dec. 22, 2010, docket No. 5 U 36/09, 2011 Beck-Rechtsprechung [BeckRS] 22463 (F.R.G.).

[106] Case C-70/10, Scarlet Extended SA v. Société Belge des auteurs, compositeurs et éditeurs (SABAM), 2011 E.C.R. I-0000.

legislator may have to amend the statutory law to bring it into conformance with EU law.[107]

In *Stichting Bescherming Rechten Entertainment Industrie Nederland (BREIN) v. Ziggo BV*,[108] the District Court of The Hague refused to issue an interim injunction against the Internet access provider Ziggo to block access to The Pirate Bay. The court presented two main arguments for its conclusion: First, in an interim proceeding, such an injunction could not be issued since it affected all of Ziggo's subscribers of which only 27% were demonstrably infringing the plaintiff's rights.[109] In light of the ECJ's decision in *L'Oréal SA v. eBay International AG*, where it was held that injunctions under IPRED article 11 also cover measures "which contribute to […] preventing further infringements of that kind,"[110] this argument has little weight. Second, the District Court of The Hague argued that the individual infringers (subscribers) would have first to be addressed directly by BREIN which would indeed have been possible since Ziggo had offered to reveal their identities upon request.[111] Significantly, no such requirement is contained in Information Society Directive article 8(3).

---

[107] See also Hans-Peter Roth, Überwachungs- und Prüfungspflichten von Providern im Lichte der aktuellen EuGH-Rechtsprechung [Surveillance and Examination Duties of Providers in Light of the Recent Case Law of the ECJ], 2012 ZEITSCHRIFT FÜR URHEBER- UND MEDIENRECHT. 125, 128 (F.R.G.).

[108] Stichting Bescherming Rechten Entertainment Industrie Nederland (BREIN)/Ziggo BV, Rechtbank's-Gravenhage [District Court of The Hague], July 19, 2010, case No. 365643, docket No. KG ZA 10-573, *available at* http://zoeken.rechtspraak.nl/resultpage.aspx?snelzoeken=true&searchtype=kenmerken&vrije_tekst=BN1445 (Neth.).

[109] *See id.* at § 4.17.

[110] Case C-324/09, L'Oréal SA v. eBay International AG, 2011 E.C.R. I-00000, § 144.

[111] Stichting Bescherming Rechten Entertainment Industrie Nederland (BREIN)/Ziggo BV, Rechtbank's-Gravenhage [District Court of The Hague], July 19, 2010, case No. 365643, docket No.

In *Nordic Records Norway AS v. Telenor ASA*,[112] a Norwegian[113] court of appeal refused to issue an injunction against the Internet access provider Telenor that would have ordered it to block access to thepriatebay.org (and other domains used by The Pirate Bay). The court did not find any infringement by Telenor itself and could not rely on any provision that specifically implemented Information Society Directive article 8(3).[114] Thus, the injunction would most likely have been issued had Information Society article 8(3) been properly transposed into Norwegian law.

In *EMI Records (Ireland) Ltd. v. UPC Communications Ireland Ltd.*,[115] the Irish High Court refused to issue an injunction against the Internet access provider UPC because Information Society Directive article 8(3) had not been transposed in Irish law and the court could thus not rely on a suitable provision of the national law.

In summary, Information Society Directive article 8 and national laws adopted pursuant to that provision have proven as a strong legal basis for website blocking

---

KG ZA 10-573, § 4.18, *available at* http://zoeken.rechtspraak.nl/resultpage.aspx?snelzoeken=true&searchtype=kenmerken&vrije_tekst=BN1445 (Neth.).

[112] Borgarting Lagmannsrett [Court of Appeal], Feb. 9, 2010, docket No. 10-006542ASK-BORG/04, *available at* http://www.it-retsforum.dk/uploads/media/Telenor_PB_dom_Borgarting_2010.pdf (Norway).

[113] Note that Norway is not a Member State of the EU. However, since it is a Member of the European Economic Area (EEA), it nonetheless has to generally implement secondary EU law. *Cf.* Agreement on the European Economic Area, art. 102, Mar. 17, 1993, 1994 O.J. (L 1) 3, 25. In particular as regards the Information Society Directive, see Decision of the EEA Joint Committee No. 110/2004 of 9 July 2004, 2004 O.J. (L 376) 45 (making the transposition of the Information Society Directive mandatory for all EEA Member States).

[114] Borgarting Lagmannsrett [Court of Appeal], Feb. 9, 2010, docket No. 10-006542ASK-BORG/04, at 31-32, *available at* http://www.it-retsforum.dk/uploads/media/Telenor_PB_dom_Borgarting_2010.pdf (Norway).

[115] EMI Records (Ireland) Ltd. v. UPC Communications Ireland Ltd., [2010] IEHC 377, *available at* http://www.bailii.org/ie/cases/IEHC/2010/H377.html.

injunctions. National courts that refused to issue an injunction mostly did so because EU law had not been properly transposed into national law. The next chapter will discuss the corresponding provision under U.S. law.

4.2 Copyright Act § 512(j)

Section 512(j)(1)(B) of the Copyright Act provides that a court may only grant injunctive relief against a service provider that qualifies for § 512(a)—i.e. typical Internet access providers or Internet backbone operators—if the injunctive relief is in on of the two following forms:

First, providers may be restrained from providing access to a particular subscriber who engaged in infringing activity and is identified in the order.[116] This scenario is not relevant here since it concerns the blocking of a user, not a website.

Second, pursuant to Copyright Act § 512(j)(1)(B)(ii), service providers may be restrained "from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States."[117] It is this provision that permits, in principle, website blocking injunctions against Internet access providers and Internet backbone operators.

Interestingly, Copyright Act § 512(j)(1)(B)(ii) has been invoked only in a single reported case: In the 2002 case of *Arista Records, Inc. v. AT&T Broadband Corp.*,[118] members of the recording industry sued to obtain an injunction against Internet backbone operators such as AT&T to enjoin them from routing any traffic to

[116] 17 U.S.C. § 512(j)(1)(B)(i).

[117] 17 U.S.C. § 512(j)(1)(B)(ii).

[118] Arista Records, Inc. v. AT&T Broadband Corp., No. 1:02CV06554, 2002 WL 34593743 (S.D.N.Y. Aug. 16, 2002).

Listen4Ever, a China-based website offering copyrighted music files for download.[119] However, the site went offline within days and the plaintiffs voluntarily withdrew their complaint.[120]

4.2.1 Requirements for an Injunction Under Copyright Act § 512(j)(1)(B)(ii)

The most critical aspect of § 512(j)(1)(B)(ii) is —in contrast to Information Society Directive article 8— that it does not provide an independent cause of action. Copyright Act § 512(j) rather states that "[t]he following rules shall apply in the case of any application for an injunction *under section 502* against a service provider."[121] Similarly the legislative history notes that § 512(j) should only apply insofar as the provider "is otherwise subject to an injunction *under existing principles of law*."[122] Furthermore, the clear purpose of the entire § 512 was to limit rather than expand liability.[123]

The plaintiffs in *Arista Records, Inc. v. AT&T Broadband Corp.* therefore misconstrued § 512(j) when they implied that Copyright Act § 512(j) could serve as

---

[119] See id. Cf. Andrews Publications, Record Labels Sue ISPs to Block Access to Chinese Web Site—Arista Records v. AT&T Broadband Corp., 20 No. 4 ANDREWS COMPUTER & ONLINE INDUS. LITIG. REP. 5 (2002).

[120] Press Release, Recording Industry Association of America, Listen4ever To Pirated Music On Chinese Web Site? Not Anymore (Aug. 21, 2002), *available at* http://www.riaa.com/newsitem.php?news_year_filter=&%20resultpage=61&id=F4367E73-FC13-62A6-94E7-81C008E5D4F1. *Cf.* Alex Pham, *Tactics Toughen on Music Piracy*, L.A. TIMES, Aug. 21, 2002, at C1, *available at* http://articles.latimes.com/2002/aug/21/business/fi-music21.

[121] 17 U.S.C. § 512(j).

[122] S. REP. 105-190, at 52 (1998) (emphasis added).

[123] S. REP. 105-190, at 40 (1998) ("New section 512 contains limitations on service providers' liability"). The Senate Report further provides that § 512(a)-(d) "also limit injunctive relief against qualifying service providers to the extent specified in subsection (i)" (which was ultimately codified as subsection (j)). *Id. a*t 40-41.

the sole statutory basis for a website blocking injunction against Internet backbone operators.[124]

The correct statutory basis for a website blocking injunction is § 512(j)(1)(B)(ii) in conjunction with § 502 of the Copyright Act. But herein lies the problem: An injunction pursuant to § 502 requires the plaintiff to show that the defendant has infringed the defendant's copyright.[125] Even if one was to construe § 502 so broadly as to allow injunctions to prevent or restrain copyright infringements by third parties irrespective of any infringements by the service provider itself, § 512 would still bar such injunctions against Internet access providers and Internet backbone operators:

Pursuant to § 512(a), injunctive relief against said providers is only available "as provided in subsection (j)."[126] As regards specifically § 512(j)(1)(B)(ii), the legislative history makes clear that an injunction pursuant to said provision is only available "in cases in which a provider is engaging in infringing activity."[127] Thus, a plaintiff has to establish copyright infringement—whether direct, vicarious, or contributory—by the Internet access provider or Internet backbone operator itself.[128]

---

[124] *See* Arista Records, Inc. v. AT&T Broadband Corp., No. 1:02CV06554, ¶ 4, 2002 WL 34593743 (S.D.N.Y. Aug. 16, 2002). *Cf.* Daniel W. Kopko, *Looking for a Crack to Break the Internet's Back: The Listen4ever Case and Backbone Provider Liability Under the Copyright Act and the DMCA*, 8 COMP. L. REV. & TECH. J. 83, 93 et seq. (2003).

[125] *See* Societe Civile Succession Richard Guino v. Int'l Found. for Anticancer Drug Discovery, 460 F. Supp. 2d 1105, 1110 (D. Ariz. 2006) ("While the issuance of an injunction is a matter of judicial discretion, such relief is not granted where the addressee of the injunction has not violated the plaintiff's copyrights and is not likely to in the future.").

[126] 17 U.S.C. § 512(a).

[127] S. Rep. 105-190, at 53 (1998).

[128] Daniel W. Kopko, Looking for a Crack to Break the Internet's Back: The Listen4ever Case and Backbone Provider Liability Under the Copyright Act and the DMCA, 8 COMP. L. REV. & TECH. J. 83, 96 et seq. (2003). But see Todd Ryan Hambidge, Containing Online Copyright Infringement:

4.2.2 Direct Infringement by the Provider

Under the RAM copy doctrine established in *MAI Systems Corp. v. Peak Computer, Inc.*,[129] it would seem easy enough to prove direct copyright infringement: Even the copy in a computer's random access memory (RAM) constitutes an actionable reproduction under the Copyright Act. When data packets containing a copyrighted work (or parts thereof) are routed through the network of an Internet access provider or Internet backbone operator, copies of these packets—and therefore copies of the protected works—are necessarily created in the RAM of the network routers operated by these providers.

However, many courts, citing *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*,[130] have held that Internet access providers and Internet backbone operators typically do "not take any affirmative action that directly result[s] in copying plaintiffs' works other than by installing and maintaining a system whereby software automatically forwards messages received from subscribers […] and temporarily stores copies on its system"[131] and therefore

---

Use of the Digital Millennium Copyright Act's Foreign Site Provision to Block U.S. Access to Infringing Foreign Websites, 60 VAND. L. REV. 905, 915 (2007) (not taking into account the legislative history and § 512(j)'s reference to § 502; thus reading § 512(j)(1)(B)(ii) as only requiring that the provider has "infringing customers").

[129] MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 518 (9th Cir. 1993). *But see* CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544, 550-51 (4th Cir. 2004); Cartoon Network LP, LLLP v. CSC Holdings, Inc., 536 F.3d 121, 129-30 (2d Cir. 2008). *Cf.* Melissa A. Bogden, *Fixing Fixation: The Ram Copy Doctrine*, 43 ARIZ. ST. L.J. 181, 203 et seq. (2011) (arguing that the RAM copy doctrine has effectively been overturned because the Fourth and Second Circuit Courts have reconciled *MAI* with a more rational approach to the fixation requirement—that it must have a durational component).

[130] Religious Tech. Ctr. v. Netcom On-Line Commc'n Services, Inc., 907 F. Supp. 1361 (N.D. Cal. 1995).

[131] *Id.* at 1368.

do not directly infringe copyright.[132] In *CoStar Group, Inc. v. LoopNet, Inc.*,[133] the Fourth Circuit endorsed *Netcom*[134] and emphasized that direct copyright infringement requires "volitional conduct."[135] The court also presented the following analogy that very well expresses the underlying reasoning:

> "[A] copy machine owner who makes the machine available to the public to use for copying is not, without more, strictly liable under § 106 for illegal copying by a customer. [The] customers pay a fixed amount per copy and operate the machine themselves to make copies. When a customer duplicates an infringing work, the owner of the copy machine is not considered a direct infringer. Similarly, an ISP who owns an electronic facility that responds automatically to users' input is not a direct infringer."[136]

In *Cartoon Network LP, LLLP v. CSC Holdings, Inc.*,[137] the 2nd Circuit, repeatedly citing *CoStar*, also endorsed *Netcom* and applied its holding to a cable television company's digital video recorder (DVR) system, which was operated by the cable

---

[132] *See* Cartoon Network LP, LLLP v. CSC Holdings, Inc., 536 F.3d 121, 132 (2d Cir. 2008); CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544, 551 (4th Cir. 2004); Ellison v. Robertson, 189 F. Supp. 2d 1051, 1056 (C.D. Cal. 2002), *aff'd in part, rev'd in part and remanded*, 357 F.3d 1072 (9th Cir. 2004); Rosen v. Hosting Services, Inc., 771 F. Supp. 2d 1219, 1222 (C.D. Cal. 2010).

[133] CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544 (4th Cir. 2004).

[134] *Id.* at 555.

[135] *Id.* at 551.

[136] Id.

[137] Cartoon Network LP, LLLP v. CSC Holdings, Inc., 536 F.3d 121 (2d Cir. 2008). For an extensive discussion see Jesse Harman, Drawing A Line Between Direct and Contributory Copyright Infringement: The Second Circuit's Take on A Copying Service Provider's Direct Liability in Cartoon Network v. Csc Holdings, 19 DEPAUL J. ART, TECH. & INTELL. PROP. L. 397 (2009).

television company's customers by remote control from their homes, but housed at a remote location.[138]

In *Ellison v. Robertson*[139] and subsequently in *Rosen v. Hosting Services, Inc.*,[140] the Central District Court of California also followed *Netcom*.

Notably, there are also cases where district courts did not require any "volitional conduct" to find direct copyright infringement. These cases have, however, not been followed by other courts and/or contain facts untypical for Internet access providers and Internet backbone operators: In the 1997 case of *Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc.*,[141] a district court found direct copyright infringement in particular because the defendant's employees viewed all uploaded files before moving them into an area generally available to subscribers.[142] In the 1993 case of *Playboy Enterprises, Inc. v. Frena*,[143] a district court held that the operator of a

[138] *See* Cartoon Network LP, LLLP v. CSC Holdings, Inc., 536 F.3d 121, 130 et seq. (2d Cir. 2008).

[139] Ellison v. Robertson, 189 F. Supp. 2d 1051, 1056 (C.D. Cal. 2002), *aff'd in part, rev'd in part and remanded*, 357 F.3d 1072 (9th Cir. 2004).

[140] Rosen v. Hosting Services, Inc., 771 F. Supp. 2d 1219, 1222 (C.D. Cal. 2010) (citing *Ellison v. Robertson*).

[141] Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc., 982 F. Supp. 503 (N.D. Ohio 1997).

[142] *Id.* at 513.

[143] Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993). The Fourth Circuit declined to follow *Frena* in CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544, 554 (4th Cir. 2004), citing H.R. REP. No. 105-551, at 11 (1998) ("As to direct infringement, liability is ruled out for passive, automatic acts engaged in through a technological process initiated by another. Thus the bill essentially codifies the result in the leading and most thoughtful judicial decision to date: *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F.Supp. 1361 (N.D.Cal.1995). In doing so, it overrules these aspects of *Playboy Enterprises, Inc. v. Frena*, 839 F.Supp. 1552 (M.D.Fla.1993), insofar as that case suggests that such acts by service providers could constitute direct infringement, and provides certainty that Netcom and its progeny, so far only a few district court cases, will be the law of the land.").

Bulletin Board System (BBS) violated the plaintiff's distribution and display rights simply by providing the space in which the plaintiff's works were uploaded and downloaded.[144]

Since neither the Ninth Circuit nor the Supreme Court itself had yet to rule on the question whether direct copyright infringement requires a "volitional" element some uncertainty still remains. However, given the cases cited above, it seems very likely that these courts, too, would also follow *Netcom*.

Thus, Internet access providers and Internet backbone operators, by routing Internet traffic alone, would not commit any direct copyright infringement. For copyright owners to obtain an injunction, vicarious or contributory infringement would therefore have to be established.

4.2.3 Vicarious Infringement by the Provider

To prove vicarious copyright infringement, a plaintiff must establish that the defendant (1) has the right and ability to supervise the infringing activity and (2) has a direct financial interest in such activities.[145] In *A&M Records, Inc. v. Napster, Inc.*, the Ninth Circuit held that the first element was met if the defendant had the "ability to block infringers' access to a particular environment for any reason whatsoever."[146]

---

[144] *See id*. at 1556-57.

[145] *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1022 (9th Cir. 2001) (quoting Gershwin Pub. Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971)); Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1173 (9th Cir. 2007) (quoting Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 930 (2005)).

[146] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001). *Cf.* Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1173 (9th Cir. 2007) (emphasizing the necessity of a "legal right to stop or limit the direct infringement").

In *Perfect 10, Inc. v. Amazon.com*, the Ninth Circuit further clarified that the defendant has to have the ability not only to stop contributing to copyright infringement (which is exclusively a question of contributory liability) but to stop the third party's direct infringement.[147] As regards Google's search engine, the court found that "Google cannot stop any of the third-party websites from reproducing, displaying, and distributing unauthorized copies of Perfect 10's images because that infringing conduct takes place on the third-party websites."[148] This very argument could also be made for Internet access providers and even Internet backbone operators: Unless the provider is able to block *all* traffic to an infringing website, it would be in no position to actually stop the infringing actions by the website's operator. Furthermore it could be argued that Internet access providers and Internet backbone operators have no contracts with infringing websites and therefore also no "right to supervise."[149]

Even if the element of "right and ability to supervise" was satisfied, the "direct financial interest" element is likely not: A direct financial interest exists "where the availability of infringing material acts as a 'draw' for customers."[150] While that "draw" does not have to be substantial,[151] it must be more than just an added

[147] *See* Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1175 (9th Cir. 2007) ("Google's failure to change its operations to avoid assisting websites to distribute their infringing content may constitute contributory liability […]. However, this failure is not the same as declining to exercise a right and ability to make third-party websites stop their direct infringement.").

[148] *Id.* at 1174.

[149] *See id. a*t 1173 ("[The plaintiff] has not shown that Google has contracts with third-party websites that empower Google to stop or limit them from reproducing, displaying, and distributing infringing copies of Perfect 10's images on the Internet.").

[150] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001) (quoting Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 263-64 (9th Cir. 1996)).

[151] Ellison v. Robertson, 357 F.3d 1072, 1078-79 (9th Cir. 2004).

benefit.[152] Thus, the plaintiff would have to establish that the defendant's customers "either subscribed because of the available infringing material or canceled subscriptions because it was no longer available."[153] This would be indeed very difficult to prove against any Internet access provider or Internet backbone operator. By routing Internet traffic alone, said providers will therefore typically not be guilty of any vicarious copyright infringement.[154]

4.2.4 Contributory Infringement by the Provider

In general, liability for contributory infringement arises where a party "with knowledge of the infringing activity, induces, causes, or materially contributes to the infringing conduct of another."[155]

Internet access providers and Internet backbone operators cannot rely on *Sony Corp. of Am. v. Universal City Studios, Inc.*[156] and argue that they should not be held liable

---

[152] Id.

[153] Ellison v. Robertson, 357 F.3d 1072, 1079 (9th Cir. 2004) (holding that there was no evidence that AOL attracted or retained subscriptions because of the infringement or lost subscriptions because of AOL's eventual obstruction of the infringement, and therefore rejecting the plaintiff's vicarious infringement claim). *Cf. also* S. REP. 105-190, at 44 (1998) ("In general, a service provider conducting a legitimate business would not be considered to receive a 'financial benefit directly attributable to the infringing activity' where the infringer makes the same kind of payment as non-infringing users of the provider's service.").

[154] Cf. Daniel W. Kopko, Looking for a Crack to Break the Internet's Back: The Listen4ever Case and Backbone Provider Liability Under the Copyright Act and the DMCA, 8 COMP. L. REV. & TECH. J. 83, 101 et seq. (2003).

[155] 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT, § 12.04[A][3][a] at 12–85 (citing Gershwin Pub. Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971)). *See also* CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544, 550 (4th Cir. 2004).

[156] Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984) (holding that "the sale of copying equipment, like the sale of other articles of commerce, does not constitute

for contributory infringement because their services (undoubtedly) have "substantial noninfringing uses."[157] This is because "substantial noninfringing uses" do not absolve from contributory liability in general but only from contributory liability claims that are based on the design of the service facilitating the infringement.[158]

As regards specifically Internet service providers, the Ninth Circuit held in *Perfect 10, Inc. v. Amazon.com, Inc.* that a computer system operator is contributorily liable if it "has actual knowledge that specific infringing material is available using its system"[159] and can "take simple measures to prevent further damage to copyrighted works, yet continues to provide access to infringing works."[160]

Internet access providers and Internet backbone operators can obtain such actual knowledge if they receive a notification by a copyright holder,[161] informing them

---

contributory infringement if the product is widely used for legitimate, unobjectionable purposes" and subsequently referring to "substantial noninfringing uses").

[157] *See* Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1170 (9th Cir. 2007) (holding that Google could not rely on *Sony* to argue against contributory liability).

[158] See id.

[159] Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1172 (9th Cir. 2007) (citing A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1022 (9th Cir. 2001)). *See also* Rosen v. Hosting Services, Inc., 771 F. Supp. 2d 1219, 1222 (C.D. Cal. 2010).

[160] Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1172 (9th Cir. 2007) (internal quotations and citations omitted; citing Religious Tech. Ctr. v. Netcom On-Line Commc'n Services, Inc., 907 F. Supp. 1361, 1375 (N.D. Cal. 1995)). *Cf.* In re Aimster Copyright Litig., 334 F.3d 643, 649 (7th Cir. 2003) (holding that the Ninth Circuit erred in A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1020 (9th Cir. 2001) in suggesting that actual knowledge of specific infringing uses is a sufficient condition for deeming a facilitator a contributory infringer). *Cf.* Mark Bartholomew & Patrick F. McArdle, *Causing Infringement*, 64 VAND. L. REV. 675, 687-88 (2011) (discussing how this broadens the material contribution standard).

[161] *Cf., e.g.,* Capitol Records. Inc. v. MP3tunes, LLC, Case No. 07 Civ. 9931, at 25 (WHP)(FM) (S.D.N.Y. Aug. 22, 2011).

about the infringing nature of a website accessible under a certain domain name or IP address.

As regards the second prong—whether a provider can take "simple measures" to prevent further infringement—it should be pointed out that one of the four factors a court has to consider when granting injunctive relief under § 512(j)(1)(B)(ii) is "whether such an injunction, either alone or in combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider's system or network."[162]

However, under the Ninth Circuit's test developed in *Perfect 10, Inc. v. Amazon.com, Inc.*, the simplicity of the measure is not just one factor to be weighed against other factors but effectively a *condition sine qua non*: To even reach the point in the analysis where the four factors are to be considered, a court first has to come to the conclusion that there are "simple measures" the service provider can take to prevent further infringement and thus is contributorily liable which requires.

Whether such "simple measures" are available to a provider depends on (1) the complexity of the technology needed to block infringing websites and (2) the extent to which such technology has already been implemented by the provider in question, even if for unrelated reasons.

The basic three methods discussed in Part 2 were DNS blocking, IP blocking, and URL blocking. DNS blocking and IP blocking require no infrastructure investments, can be maintained centrally and with very little cost to the service provider. Thus,

[162] 17 U.S.C. § 512(j)(2)(A).

these two methods have to be considered “simple measures” irrespective of whether the service provider in question has implemented them before.

URL blocking on the other hand requires a network infrastructure that is capable of analyzing all user's web traffic. To implement this functionality, substantial investments are needed. Thus, URL blocking cannot generally be considered a "simple measure." However, if service providers have already implemented a URL blocking system for other reasons—such is the case in the UK[163]—the blocking of an additional URL would be "simple" since it did not require any infrastructure investments.

In summary, there is a prima facie case of contributory copyright infringement by an Internet access provider if it does not perform any DNS blocking or IP blocking of websites of which the service provider has actual knowledge that they infringe copyright. The same applies to backbone operators as regards IP blocking.

4.2.5 Factors to Consider Before Issuing an Injunction

Pursuant to Copyright Act § 512(j)(2), a court has to consider the following four factors in determining whether to grant injunctive relief pursuant to § 512(j):

First, it has to be considered whether the injunction would "significantly burden either the provider or the operation of the provider's system or network."[164] The substance of this factor already had to be considered in determining whether the

[163] In the UK, most Internet access providers, in cooperation with the Internet Watch Foundation (IWF), currently perform URL blocking to constrain access to abusive images of children. *See* UK OFFICE OF COMMUNICATIONS, "SITE BLOCKING" TO REDUCE ONLINE COPYRIGHT INFRINGEMENT 36 (2011), *available at* http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf.

[164] 17 U.S.C. § 512(j)(2)(A).

service provider was contributorily liable (i.e. could take "simple measures" to prevent further damage to copyrighted works) which, as discussed *supra* in Part 4.2.1, is a precondition for an injunction. However, this does not mean that this factor is irrelevant in comparison to the other three factors. This is because the "simple measure"-test that has to be met to find contributory infringement is an absolute one while in the context of Copyright Act § 512(j)(2), the burden on the service provider is relative and has to be considered in light of the other three factors. For example, if the copyrighted work in question has no commercial value, is made illegally available on a website that only has very few visitors, and is simultaneously published by the copyright holder on another website (i.e. is not an unpublished work), even the "simple measure" of implementing IP blocking in a network in which this functionality has not been pre-configured, may be too much of a burden on the service provider.

In this context it has to be noted that it should not be considered a burden on the enjoined Internet access provider that it might lose customers (and thus revenue) because some customers wish to continue to use the infringing website. This is because the loss of profits otherwise made due to contributory copyright infringement can hardly be considered relevant under Copyright Act § 512(j)(2).[165]

The second factor is the "magnitude of the harm likely to be suffered by the copyright owner" if steps are not taken to prevent or restrain the infringement.[166] This necessitates that the court considers evidence regarding the commercial value

[165] But see Todd Ryan Hambidge, Containing Online Copyright Infringement: Use of the Digital Millennium Copyright Act's Foreign Site Provision to Block U.S. Access to Infringing Foreign Websites, 60 VAND. L. REV. 905, 918 (2007).

[166] 17 U.S.C. § 512(j)(2)(B).

of the copyrighted work at issue as well as the amount of profits likely lost due to the infringement committed by the operator and the users of the website in question.[167]

Third, a court has to consider whether the implementation of such an injunction would be "technically feasible and effective,"[168] and "would not interfere with access to noninfringing material at other online locations."[169] The feasibility has to be affirmed not only for DNS blocking and IP blocking but also for URL blocking.[170] As regards the effectiveness of these measures, the ease of circumvention has to be considered. As discussed in Part 2, IP blocking can be circumvented easily by the operator of the website in question and DNS blocking is only a small obstacle for determined users. Only circumvention of URL blocking would be significantly more difficult.

However, the question is not whether the website's operator and/or the users could circumvent the blocking but (1) how many users—or in the case of IP blocking, whether the website operator—would actually do so and (2) how long it would take them to perform the circumvention. For example, if (only) 50% of the users would bother to circumvent the blocking, it may still be considered sufficiently effective if the copyrighted work in question has a significant commercial value.

---

[167] Cf. Todd Ryan Hambidge, Containing Online Copyright Infringement: Use of the Digital Millennium Copyright Act's Foreign Site Provision to Block U.S. Access to Infringing Foreign Websites, 60 VAND. L. REV. 905, 919 (2007).

[168] 17 U.S.C. § 512(j)(2)(C).

[169] Id.

[170] *Cf.* UK OFFICE OF COMMUNICATIONS, "SITE BLOCKING" TO REDUCE ONLINE COPYRIGHT INFRINGEMENT 36 (2011), *available at* http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf (noting that most Internet access providers in the UK perform URL blocking to constrain access to abusive images of children).

The third factor also refers to the interference with access to noninfringing material at other online locations. This concerns the precision with which the blocking is performed. As discussed *supra* in Part 2, IP blocking carries with it the risk of blocking other websites that happen to share an IP address with the blocked website. DNS blocking has a smaller but still substantial risk of overbreadth. URL blocking is clearly the most precise but, of course, also the most burdensome for the service provider.[171]

Fourth, it has to be considered whether "other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available."[172] The primary alternative to a website blocking injunction, is of course, a lawsuit against the operator of the website in question. This factor will weigh strongly in the plaintiff's favor if he can show that he would have to bring suit in a jurisdiction where there is no comparable body of copyright law or where the judicial process is corrupt or overly long.

In light of the four factors discussed above, copyright holders will be able to obtain a website blocking injunction in particular to force IP blocking or DNS blocking of websites that provide only one type of content to users: download links to copyrighted works made available without authorization. The burden on the service provider caused by this injunction would be negligible while the magnitude of the harm likely to be suffered by the copyright owner would otherwise typically be substantial. If the website has its own domain, DNS blocking would not interfere

[171] Cf. Todd Ryan Hambidge, Containing Online Copyright Infringement: Use of the Digital Millennium Copyright Act's Foreign Site Provision to Block U.S. Access to Infringing Foreign Websites, 60 VAND. L. REV. 905, 924 (2007).

[172] 17 U.S.C. § 512(j)(2)(D).

with access to noninfringing material. If it has its own IP address, IP blocking would also not constitute such interference. However, if the website has neither its own domain name nor its own IP address, there would likely be substantial interference with noninfringing material when IP blocking or DNS blocking was performed. In particular in such situations, URL blocking would be most precise. However, due to the burden on the service provider of implementing a URL blocking system, an injunction that can only be complied with by implementing URL blocking would only be appropriate if the service provider in question has already implemented such a system.

5. A Comparative Analysis

The following chapters provide a comparative analysis between Copyright Act § 512(j) and article 8 of the Information Society Directive. Part 5.1 will discuss the relationship between the service provider's potential copyright infringement and a blocking injunction. Parts 5.2 and 5.3 will, respectively, describe the territorial and personal scope of application while Part 5.4 will address the issue of specificity of an injunction. Lastly, Part 5.5 will analyze the fundamental rights and proportionality considerations of Copyright Act § 512(j) and Information Society Directive article 8.

5.1 Do the Service Provider's Actions Have to Constitute Prima Facie Infringement?

Article 8(3) of the Information Society Directive provides that an injunction can be issued against intermediaries if their services "are used by a third party to infringe a copyright or related right."[173] Thus, as already discussed *supra* in Part 4.1, service

[173] Information Society Directive art. 8(3).

providers do not have to infringe any copyright for a website blocking injunction to be issued against them.

Contrary to that, a website blocking injunction under Copyright Act §§ 512(j), 502 requires that the service provider infringed the plaintiff's copyright. This requirement may be a significant contributing factor to the unwillingness of copyright holders to seek website blocking injunctions in the U.S. As shown *supra* in Part 4.2, establishing copyright infringement by the service provider is possible but ultimately based on a theory of contributory infringement which is a rather complex area of law that is still very much evolving. In this respect, the legal situation in the EU provides right holders with much more legal certainty.

5.2 Territorial Scope of Application

Naturally, both EU and U.S. law only apply to service providers operating in the respective jurisdiction. The interesting issue is that of the territorial scope of indirect application, i.e. which websites are potentially subject to blocking?

Section 512(j) of the Copyright Act explicitly answers this question by referring specifically to an “online location outside the United States.”[174] The legislative history reiterates this point by stating that "blocking orders are not available […] in the case of infringing activity on a site within the United States or its territories."[175]

Information Society Directive article 8, on the other hand, provides no indication as to which websites should be subject to potential blocking. From this it seems to follow that, in principle, a service provider operating in a Member State might be

[174] 17 U.S.C. § 512(j)(1)(B)(ii).

[175] S. REP. 105-190, at 53 (1998).

obligated to block (1) websites located outside of the territory of the EU, (2) websites located in the EU but outside of the territory of the Member State in which the service provider operates in; and (3) websites located in the same Member State as the service provider.

In this context, recital 59 of the Information Society Directive has to be considered. It states that the reason for allowing injunctions against intermediaries such as service providers was that, "[i]n many cases, such intermediaries are best placed to bring such infringing activities to an end."[176] In light of this rationale for injunctions against intermediaries, Information Society Directive article 8 has to be construed as only to permit an injunction against an intermediary if it is indeed "best placed to bring [the] infringing activities to an end."[177] Thus, right holders are required to at least establish that an alternative to an injunction against a service provider would be impractical or less effective.[178]

Effectively, this means that Information Society Directive article 8 can rarely serve as a legal basis for injunctions requiring the blocking of a website located in the same Member State as the Internet access provider or backbone operator itself: The operator of the website in question or its hosting provider would be able to block access to the infringing content not only more effectively but also more efficiently than any Internet access provider or Internet backbone operator.

---

[176] Information Society Directive recital 59.

[177] Id.

[178] *But see* Oberlandesgericht [OLG] [Superior Regional Court] Wien, Nov. 14, 2011, docket No. 1 R 153/11v, at 17 (Austria) (holding that the right to obtain a website blocking injunction was not subordinate to any other remedy that might be available against any third party, e.g. against the operator of the infringing website).

As regards websites located within the EU but in a different Member State than the service provider, the critical question is how difficult it is for the right holder to obtain and enforce an injunction against the out-of-state website operator.

Pursuant to Council Regulation No. 44/2001[179] (hereinafter *Brussels I Regulation*), "in matters relating to tort, *delict* or *quasi-delict*,"[180] a person domiciled in a Member State may be sued "in the courts for the place where the harmful event occurred or may occur."[181] Copyright infringement constitutes such a tort or delict and is therefore covered by this provision.[182]

The ECJ has held that this wording is "intended to cover both the place where the damage occurred and the place of the event giving rise to it, so that the defendant may be sued, at the option of the claimant, in the courts for either of those places."[183] Furthermore, the "place where the damage occurred" has to be interpreted as "the place where the damage […] actually manifests itself."[184] Thus, a right

[179] 2001 O.J. (L 12) 1 (EC), as amended.

[180] Brussels I Regulation art. 5(3) (emphasis in original).

[181] *Id*.

[182] *See* Bundesgerichtshof [BGH] [Federal Court of Justice] Feb. 15, 2007, 171 Entscheidungen des Bundesgerichtshofes in Zivilsachen [BGHZ] 151 (F.R.G.); Cass. 1e civ., July 16, 1997, Bulletin d'information de la Cour de Cassation 1997 No. 245, at 164 (Fr.); Oberster Gerichtshof [OGH] [Supreme Court] July 13, 1999, 4 Ob 347/98b, 1999 Zeitschrift für Rechtsvergleichung [ZfRV] No. 83 (Austria). *Cf. also* WORLD INTELLECTUAL PROPERTY ORGANIZATION [WIPO], INTELLECTUAL PROPERTY ON THE INTERNET: A SURVEY OF ISSUES 123 (2002), *available at* http://www.wipo.int/export/sites/www/copyright/en/ecommerce/pdf/survey.pdf.

[183] Case C-189/08, Zuid-Chemie BV v. Philippo's Mineralenfabriek NV/SA, 2009 E.C.R. I-06917, § 23.

[184] *Id.* at § 27 (referring to Case C-68/93 Shevill v. Presse Alliance SA, 1995 E.C.R. I-415, § 21).

holder effectively may sue in any Member State in which its rights are infringed.[185] As regards specifically "provisional, including protective measures" such as preliminary injunctions,[186] a right holder can claim either one of the aforementioned jurisdictions under the Brussels I Regulation or a jurisdiction under national law.[187] Once obtained, the judgment is enforceable in all Member States.[188] Moreover, pursuant to article 8 of Parliament and Council Regulation 864/2007[189] (hereinafter *Rome II Regulation*), the *lex loci protectionis* ("the law of the country for which protection is claimed")[190] applies in copyright litigations.[191]

Furthermore, there exists also another reason why website blocking injunctions against local service providers may be more efficient than an injunction against the website operator: Website blocking injunctions apply to a particular website, irrespective of the website's operator. An injunction against a website operator, on

[185] *Cf.* Reinhold Geimer & Rolf A. Schütze, Europäisches Zivilverfahrensrecht [European Civil Procedure Law] 237-8 (3rd ed. 2010).

[186] *Cf.* Case C-261/90, Reichert v. Dresdner Bank AG, 1992 E.C.R. I-02149, § 34 (holding that the expression "provisional, including protective, measures" is to be understood as "referring to measures which, in matters within the scope of the Convention, are intended to preserve a factual or legal situation so as to safeguard rights the recognition of which is sought elsewhere from the court having jurisdiction as to the substance of the matter").

[187] *See* Brussels I Regulation art. 31. *Cf.* REINHOLD GEIMER & ROLF A. SCHÜTZE, EUROPÄISCHES ZIVILVERFAHRENSRECHT [EUROPEAN CIVIL PROCEDURE LAW] 561 (3rd ed. 2010). That preliminary injunctions fall within the scope of the Brussels I Regulation has long been established. *See* Case 120/79, Louise de Cavel v. Jacques de Cavel, 1980 E.C.R. 731, § 12.

[188] *See* Brussels I Regulation art. 38.

[189] 2007 O.J. (L 199) 40 (EC).

[190] Rome II Regulation art. 8(1).

[191] *Cf. id.* recital 26 (stating that "[r]regarding infringements of intellectual property rights, the universally acknowledged principle of the lex loci protectionis should be preserved"). *Cf. also* CHRISTIAN HEINZE, EINSTWEILIGER RECHTSSCHUTZ IM EUROPÄISCHEN IMMATERIALGÜTERRECHT [PRELIMINARY REMEDIES UNDER EUROPEAN INTELLECTUAL PROPERTY LAW] 337 (2007).

the other hand, can only be enforced against that specific operator. If the operator sells or otherwise transfers the website to another entity, the injunction could effectively not be enforced. This problem is, of course, exacerbated by the long time it takes to transmit and serve judicial documents in other Member States.

Thus, in theory, it is easily possible to obtain and enforce an injunction against a website operator located in a different Member State. However, in practice, it takes one to three months, and in some cases up to six months, to transmit and serve judicial documents in other Member States.[192] This is particularly relevant since article 34 of the Brussels I Regulation provides that a judicial decision is not recognized and enforced in another Member State if the defendant was not served with the relevant judicial document in such a way as to enable him to arrange for his defense.[193] Thus, a potentially time-consuming service on the defendant is necessary for a preliminary injunction to be recognized and enforceable in another Member State.

Thus, even if the website in question is located in the EU but in a different Member State, local Internet access providers and Internet backbone operators may still be

[192] *See* Commission report on the application of Council Regulation (EC) 1348/2000 on the service in the Member States of Judicial and Extrajudicial documents in civil or commercial matters, at 4, COM (2004) 603 final, Oct. 1, 2004,

[193] *See* Brussels I Regulation art. 34(2). Note that there is only one exception to the requirement of prior service: if the defendant "failed to commence proceedings to challenge the judgment when it was possible for him to do so." *Id.* This is to be interpreted as meaning that "it is 'possible' for a defendant to bring proceedings to challenge a default judgment against him only if he was in fact acquainted with its contents, because it was served on him in sufficient time to enable him to arrange for his defence before the courts of the State in which the judgment was given." Case C-283/05, ASML Netherlands BV v. Semiconductor Industry Services GmbH (SEMIS), 2006 E.C.R. I-12041, § 49.

"best placed to bring […] infringing activities to an end."[194] Injunctions pursuant to Information Society Directive article 8 will therefore generally be available to force the blocking of a website located in another Member State.

This is not only in line with national court cases discussed *supra* in Part 4.1.2 in which website blocking injunctions were granted to block the Swedish website The Pirate Bay[195] but also does not violate the country of origin principle set out in article 3 of the E-Commerce Directive.

The country of origin principle as codified in E-Commerce Directive article 3 provides that Member States "may not, for reasons falling within the coordinated field, restrict the freedom to provide information society services from another Member State."[196] Thus, a Member States must generally ensure that, in relation to the broadly defined "coordinated field,"[197] a service provider "is not made subject to stricter requirements than those provided for by the substantive law applicable in the Member State in which that service provider is established."[198] The country of origin principle therefore serves the purpose of reducing "legal obstacles to the proper

[194] Information Society Directive recital 59.

[195] *See* Hof van Beroep [Court of Appeal] Antwerpen, Sept. 26, 2011, docket No. 2011/8314 (Belgium), *available at* http://nurpa.be/files/20111004_BAF-Belgacom-Telenet-DNS-blocking.pdf; Højesterets [Supreme Court], May 27, 2010, docket No. 153/2009, *available at* http://www.domstol.dk/hojesteret/Documents/Domme/153-09.pdf (Denmark); Cass., sez. III penale, Sept. 29, 2009, n.49437/09 (Italy), *available at* http://blog.quintarelli.it/files/cassazione-sentenza-49437-2009.pdf.

[196] E-Commerce Directive art. 3(2).

[197] *See* E-Commerce Directive art. 2(h) (defining "coordinated field" as "requirements laid down in Member States' legal systems applicable to information society service providers or information society services, regardless of whether they are of a general nature or specifically designed for them").

[198] Joined Cases C‑509/09 and C‑161/10, 2011 E.C.R. I-0000, § 68.

functioning of the internal market which make less attractive the exercise of the freedom of establishment and the freedom to provide services."[199]

However, pursuant to E-Commerce Directive article 3(2), the country of origin principle does not apply to the fields of law referred to in the directive's annex. Among the fields specifically listed in the annex is "copyright," including neighboring rights.[200] Thus, it is in full compliance with the E-Commerce Directive, that pursuant to Information Society Directive article 8, website blocking injunctions can be obtained to block a website located in another Member State.

Lastly, as regards websites located outside of the EU, local Internet access providers and Internet backbone operators are clearly "best placed to bring […] infringing activities to an end."[201]

In summary, Information Society Directive article 8(3) applies to websites located outside of the EU but also to website located inside the EU if they are in different Member State than that of the Internet access provider or backbone operator being sued. In this respect, Information Society Directive article 8(3) differs significantly from Copyright Act § 512(j) which only applies to websites located outside of the United States but not to websites that are located just in a different state than the Internet access provider or backbone operator.

[199] E-Commerce Directive recital 5.

[200] *See* annex of the E-Commerce Directive, first indent. Note that naturally the country of origin principle does also not apply in the legal areas which are exempted entirely from the directive's scope, such as data protection. *See* E-Commerce-Directive art. 1(5).

[201] Information Society Directive recital 59.

5.3 Personal Scope of Application

Neither Information Society Directive article 8(3) nor Copyright Act § 512(j) explicitly state whether website blocking injunctions can only be obtained against Internet access providers or also against Internet backbone operators.

As discussed *supra* under Part 4.1, Information Society Directive article 8(3) uses the term "intermediary" and covers any type of provider "who carries a third party's infringement of a protected work or other subject-matter in a network."[202] Thus, under EU law, website blocking injunctions are also available against Internet backbone operators.

Similarly, Copyright Act § 512(j) applies to all service providers covered by § 512(a), therefore to typical Internet access providers as well as Internet backbone operators.[203] Significantly, the only case brought so far under § 512(j)(1)(B)(ii) concerned exclusively Internet backbone operators.[204]

5.4 Required Specificity of the Injunction

An Injunction pursuant to Information Society Directive article 8(3) must not amount to a "general" monitoring obligation.[205] As discussed under Part 4.1.1, this prohibits injunctions requiring the monitoring of "all the data relating to each of [the

[202] Information Society Directive recital 59.

[203] *See supra* Part 4.2.

[204] *See* Arista Records, Inc. v. AT&T Broadband Corp., No. 1:02CV06554, 2002 WL 34593743 (S.D.N.Y., Aug. 16, 2002). *Cf. supra* Part 4.2.

[205] *See* E-Commerce Directive art. 15(1).

service provider's] customers."[206] Thus, an injunction to block any and all websites that make the plaintiff's copyrighted works available is impermissible since it would require general traffic monitoring. However, whether an injunction could effectively require a service provider to perform a daily web search in order to identify and subsequently block websites that host a particular infringing content is unclear.

Under Copyright Act § 512(j), this issue is addressed in a much more straightforward fashion. § 512(j)(1)(B)(ii) only permits an injunction to block access to "a specific, identified, online location."[207] Since the term "online location" describes a technical construct, a technical identifier is necessary. On the World Wide Web, there are only three possible means by which an online location can be technically identified: an IP address (e.g. 192.0.43.10), a domain name (e.g. www.example.com), or a URL (e.g. http://www.example.com/~jdoe/movies.html). Of course, a URL is significantly more specific than a domain name which in turn is significantly more specific than an IP address. This is due to the fact that one IP address can be used to host hundreds of domain names and one domain can be used for countless separate sites, each with its own URL. Nonetheless, as regards the required specificity of a website blocking injunction, Copyright Act § 512(j) provides an extent of legal clarity that is lacking from Information Society Directive article 8(3).

[206] Case C-70/10, Scarlet Extended SA v. Société Belge des auteurs, compositeurs et éditeurs (SABAM), 2011 E.C.R. I-0000, § 40.

[207] Copyright Act § 512(j)(1)(B)(ii).

5.5 Fundamental Rights and Proportionality Considerations

The following sections will focus on specific fundamental rights issues that highlight the differences and similarities between Copyright Act § 512(j) and Information Society Directive article 8(3).

5.5.1 Whether to Consider Free Speech Rights and Over-Blocking

Information Society Directive article 8 does not explicitly take into account any free speech aspects.[208] However, IPRED article 3 specifically requires that all enforcement measures be "proportionate."[209] Specifically, in *Scarlet Extended SA v. Société Belge des auteurs, compositeurs et éditeurs (SABAM)*, the ECJ has held that the protection of the right to intellectual property has to be balanced with other fundamental rights[210] such as the freedom to receive or impart information.[211] This follows from the fact that the Charter of Fundamental Rights of the European Union[212] (hereinafter *EU Charter*) protects the right to intellectual property[213] as

[208] Indeed, the entire directive makes no note of the fundamental rights issues concerning blocking injunctions.

[209] IPRED art. 3(2). *Cf. also* Case C-70/10, Scarlet Extended SA v. Société Belge des auteurs, compositeurs et éditeurs (SABAM), 2011 E.C.R. I-0000, § 36 (referring to Case C-324/09, L'Oréal SA v. eBay International AG, 2011 E.C.R. I-00000, § 139).

[210] *See* Case C-70/10, Scarlet Extended SA v. Société Belge des auteurs, compositeurs et éditeurs (SABAM), 2011 E.C.R. I-0000, § 44 (referring to Case C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 2008 E.C.R. I-00271, §§ 62-68).

[211] *See id.* at §§ 50, 52.

[212] 2010 O.J. (C 83) 389 (EU).

[213] *See* EU Charter art. 17(2).

well as the freedom of expression and the freedom of information[214] without making any of these fundamental rights inviolable.[215]

Since many potentially blocked websites are operated by non-EU-citizens from third countries, it is highly significant whether the freedom of expression as protected under the EU Charter also applies to foreigners. Following the approach of the Convention for the Protection of Human Rights and Fundamental Freedoms[216] (hereinafter *ECHR*), the EU Charter protects the rights of "everyone," i.e. of every human being, without "any discrimination on grounds of nationality."[217]

Thus, in the context of Information Society Directive article 8(3), the free expression interests of foreign website operators and the interests of EU website operators are equally relevant. Proportionality has therefore to be maintained between their legitimate interests and the interests of right holders seeking an injunction.

---

[214] *See* EU Charter art. 11(1).

[215] *Cf.* Scarlet Extended SA v. Société Belge des auteurs, compositeurs et éditeurs (SABAM), 2011 E.C.R. I-0000, § 43.

[216] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 11, 1950, Council of Europe CETS No. 005, 213 U.N.T.S. 222. In addition to the EU Charter, the ECJ may also rely on the "constitutional traditions common to the Member States" as a legal basis for fundamental rights. *See* art. 6(3) of the Treaty on European Union, Dec. 29, 2006, 2006 O.J (C 321 E) 5. Since all Member States have ratified the ECHR, it may still be relied upon by the ECJ. Furthermore, the EU itself will also ratify the ECHR. *See* TEU art. 6(2).

[217] EU Charter art. 21(2). *Cf. also* Charsten Nowak, *Grundrechtsberechtigte und Grundrechtsadressaten* [*Subjects and Addressees of Fundamental Rights*], *in* HANDBUCH DER EUROPÄISCHEN GRUNDRECHTE [HANDBOOK OF THE EUROPEAN FUNDAMENTAL RIGHTS] 212, 216 (Sebastian Heselhau & Carsten Nowak eds., 2006). Specifically as regards the freedom of speech and the freedom of information, cf. Jürgen Kühling, *Kommunikationsfreiheit (Meinungsäußerungs- und Informationsfreiheit)* [*Freedom of Communication (Freedom of Speech and Information)*], *in* HANDBUCH DER EUROPÄISCHEN GRUNDRECHTE [HANDBOOK OF THE EUROPEAN FUNDAMENTAL RIGHTS] 648, 663 (Sebastian Heselhau & Carsten Nowak eds., 2006).

In cases where a website operator exclusively makes copyright-infringing content available, it will be easy to satisfy this proportionality requirement. However, if a blocking injunction affects multiple website operators of which only one made copyright-infringing information available, an injunction would likely be disproportionate as regards the non-infringing website operators. They would be prevented from communicating with certain users simply because they happened to unknowingly share a technical resource (e.g. an IP address) with a copyright infringer.

In contrast to Information Society Directive article 8(3), Copyright Act § 512(j) explicitly takes free speech considerations into account: Section 512(j)(2)(C) states that, before granting injunctive relief, a court has to consider "whether implementation of such an injunction […] would not interfere with access to noninfringing material at other online locations."[218] This wording that focuses on the users' ability to access websites rather than the (foreign) website operators' ability to reach users is reflective of the interpretation of the First Amendment.

In stark contrast to EU law and the ECHR, U.S. constitutional law generally does not protect the freedom of expression of foreigners when they reside outside of the United States.[219] This means that since Copyright Act § 512(j)(1)(B)(ii) only applies

[218] Copyright Act § 512(j)(2)(C).

[219] *Cf.* U.S. ex rel. Turner v. Williams, 194 U.S. 279, 292 (1904) ("It is, of course, true, that if an alien is not permitted to enter this country […] he is in fact cut off from worshipping or speaking or publishing or petitioning in the country"); DKT Mem'l Fund Ltd. v. Agency for Int'l Dev., 887 F.2d 275, 284 (D.C. Cir. 1989) (holding that, in principle, "aliens beyond the territorial jurisdiction of the United States are generally unable to claim the protections of the First Amendment"); Am.-Arab Anti-Discrimination Comm. v. Reno, 70 F.3d 1045, 1064 (9th Cir. 1995) (“freedom of speech and of press is accorded aliens *residing in this country*”) (emphasis added) (quoting Bridges v. Wixon, 326 U.S. 135, 148 (1945)). *Cf. also* Timothy Zick, *The First Amendment in Trans-Border Perspective: Toward A More Cosmopolitan Orientation*, 52 B.C. L. REV. 941, 944 (2011) (noting that "[a]s far as

to online locations outside of the U.S. in the first place, the free speech interests of operators of blocked websites are generally unprotected by the First Amendment to the U.S. Constitution.[220] However, the interests of users in the U.S. who may want to access these (foreign) websites are, at least partially,[221] protected under the First Amendment.[222]

However, it is noteworthy that the statute only refers to "access to noninfringing material at *other online locations*."[223] This would indicate that the users' interests in accessing noninfringing material at the *same online location* are not a significant factor. However, since the list of factors provided by Copyright Act § 512(j)(2) is not exhaustive,[224] a court should also consider whether the injunction would interfere with access to noninfringing material at the *same online location*. For example, if only a small fraction of the material made available by a website is infringing, a court should take into account the users' First Amendment-protected interests to receive noninfringing information provided by the same website.

---

alien speakers and audiences are concerned, there appears to be little support for applying the First Amendment extraterritorially").

[220] Cf. Todd Ryan Hambidge, Containing Online Copyright Infringement: Use of the Digital Millennium Copyright Act's Foreign Site Provision to Block U.S. Access to Infringing Foreign Websites, 60 VAND. L. REV. 905, 927 (2007) (noting that "the freedom of speech will not be implicated because the provision prevents speech in a foreign location (not subject to U.S. law)").

[221] *See* Meese v. Keene, 481 U.S. 465, 480 (1987) (upholding limits on distribution of foreign "political propaganda" in the U.S.). *Cf.* Timothy Zick, *The First Amendment in Trans-Border Perspective: Toward A More Cosmopolitan Orientation*, 52 B.C. L. REV. 941, 950 et seq. (2011).

[222] *See* Lamont v. Postmaster Gen., 381 U.S. 301, 305 (1965) (invalidating a prior restraint requiring a recipient of foreign propaganda to affirmatively request delivery).

[223] Copyright Act § 512(j)(2)(C) (emphasis added).

[224] *See* S. REP. 105-190, at 53 (1998) (stating that subsection (2) "sets forth mandatory considerations for the court *beyond those that exist under current law*" (emphasis added)).

In sum, both Copyright Act § 512(j) and Information Society Directive article 8(3) take free speech considerations into account. Copyright Act § 512(j) does so explicitly while Information Society Directive article 8(3) does so only when interpreted in accordance with IPRED article 3. Thus, Information Society Directive article 8(3) requires that the users' interests in accessing potentially blocked websites are considered as well as the freedom of expression interests of the foreign website operators. In comparison to that, Copyright Act § 512(j), as construed in accordance with the First Amendment, only takes the users' but not the website operators' interests into account.

5.5.2 Whether to Consider the Burden on the Provider

Information Society Directive article 8(3) does not explicitly require that the burden on the Internet access provider or backbone operator against which the injunction is issued be considered by the court. However, IPRED article 3(1) has to be taken into account which requires that all measures be proportional and "not […] unnecessarily complicated or costly."[225] In *Scarlet Extended SA v. Société Belge des auteurs, compositeurs et éditeurs (SABAM)*, the ECJ has also held that injunctions that force service providers to block certain traffic at their own expense interfere with the service providers' fundamental freedom to conduct a business which is protected by article 16 of the EU Charter.[226] Thus, "courts must […] strike a fair balance between

[225] IPRED art. 3(1). *Cf.* Case C-70/10, Scarlet Extended SA v. Société Belge des auteurs, compositeurs et éditeurs (SABAM), 2011 E.C.R. I-0000, § 48.

[226] *See id.* at § 46. *Cf. also* Case C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV, 2012 E.C.R. I-0000, § 44 (holding the same with regard to a hosting provider).

the protection of the intellectual property right enjoyed by copyright holders and that of the freedom to conduct a business enjoyed by [service providers]."[227]

In *Scarlet Extended SA v. SABAM*, the ECJ found that an obligation to install a system, at the service provider's own cost, that would have to filter the entire Internet traffic of all users did not strike such a "fair balance" and would thus infringe the service provider's freedom to conduct a business.[228] Similarly, it can be argued that URL blocking is disproportionately costly, in particular in consideration of the significantly less expensive alternatives of DNS blocking and IP blocking.

Copyright Act § 512(j) explicitly requires that it be taken into account whether "other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available."[229] Thus, § 512(j) generally leads to the same result as Information Society Directive article 8(3): DNS blocking and IP blocking are less burdensome for the service provider but, in particular in combination, comparably effective to URL blocking. Thus, an injunction can generally only require a service provider to perform DNS blocking and/or IP blocking but not URL blocking.

5.5.3 How to Quantify the Copyright Holder's Interests

As discussed *supra* in Parts 5.5.1 and 5.5.2, Information Society Directive article 8(3) requires that the copyright holder's interests are balanced against the interests of users and website operators who want to freely receive or impart

[227] Case C-70/10, Scarlet Extended SA v. Société Belge des auteurs, compositeurs et éditeurs (SABAM), 2011 E.C.R. I-0000, § 46.

[228] *See id.* at 54.

[229] 17 U.S.C. § 512(j)(2)(D).

information as well as against the service provider's interest to freely conduct its business. This raises the question of how to quantify the copyright holder's interests, in particular in light of the often questioned[230] effectiveness of website blocking measures.

The effectiveness of blocking measures should not only be considered relevant because it aides in determining the copyright holder's interest in obtaining the injunction but also because IPRED article 3(2) explicitly requires that all measures adopted pursuant to the directive be "effective."[231]

As discussed in Part 2, DNS blocking can be circumvented rather easily by users while IP blocking can be circumvented rather easily by website operators. Thus, even in combination, these measures are in no way perfect. However, the correct measure of effectiveness is not whether they *can* be circumvented but rather whether they *will* be circumvented. Furthermore, the interest of the copyright holder should not be determined by the number of users who will perform a circumvention; rather, it is the number of potentially interested users who will *not* circumvent the blocking—and will thus be prevented from accessing the infringing website—that should be used to quantify the copyright holder's interest in obtaining the injunction.[232]

---

[230] *Cf., e.g.,* Steve Crocker et al., Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill 7 (2011), http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf.

[231] IPRED art. 3(2).

[232] Cf. Stephan Steinhofer & Lukas Feiler, Urheberrechtliche Ansprüche auf die Sperrung von Websites durch Access-Provider [Claims Under Copyright Law for the Blocking of Websites by Internet Access Providers], 2010 MEDIEN UND RECHT 322, 325 (Austria).

None of the European court decisions so far have formulated any such specific measure of the copyright holder's interests. Nevertheless, adopting a similar reasoning as above, the British High Court has held in *Twentieth Century Fox Film Corp. v. British Telecommunications PLC* that even preventing only a minority of users from accessing the website can be sufficient to justify the interference with the users' and the service provider's rights.[233]

Copyright Act § 512(j)(2) explicitly states that, before issuing an injunction, it has to be considered "whether implementation of such an injunction would be […] effective."[234] Furthermore, another factor to be considered is "the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement."[235] To determine that magnitude of harm, it is necessary to estimate how many users would access the infringing website but would be prevented from doing so if the injunction was issued. From this it follows that Copyright Act § 512(j), too, requires the effectiveness of the blocking measure to be taken into account the same way as under Information Society Directive article 8(3).

Both Information Society Directive article 8(3) and Copyright Act § 512(j) require the consideration of the number of effectively blocked users that would otherwise potentially access the website. Since that number of users will be proportionally

[233] Twentieth Century Fox Film Corp. v. British Telecommunications PLC, [2011] EWHC 1981 (Ch.), July 28, 2011, at § 198, *available at* http://www.bailii.org/ew/cases/EWHC/Ch/2011/1981.html (U.K.). *Cf. also* Byret [City Court] Copenhagen, Oct. 25, 2006, docket No. F1-15124/2006, *available at* http://www.dr.dk/NR/rdonlyres/EF2AAB7A-0E04-4963-963A-463CD7550D72/361965/tele2_ke.pdf (Denmark).

[234] Copyright Act § 512(j)(2)(C).

[235] Copyright Act § 512(j)(2)(B).

higher for larger service providers, it can be generally observed that website blocking injunctions are more likely to be granted against large service providers than smaller ones. This is only fair since larger service providers will find it much easier to absorb the fixed costs of implementing a blocking measure.

6. The Effects of Website Injunctions—The Death of the Global Internet or the Emergence of the Rule of Law?

The Internet is a decentralized global communications infrastructure that is based on a set of common protocols and common resource identifiers such as domain names and IP addresses. This means that a certain domain name or IP address can be used anywhere in the world, by using any computer connected to the Internet, establishing a connection with the same server. Specifically as regards domain names, this principle has recently been termed "domain name universality."[236] It effectively means that there is a single global Internet that does not look or behave differently, depending on one's location.

Content providers have long ago started to differentiate between users depending on their location, the most recent and most obvious example being location-based mobile services. The Internet's global infrastructure has, however, so far been ignorant of a user's location, providing the same Internet to everybody. Notable exceptions are countries that engage in centralized content filtering at the level of Internet access providers or Internet backbone operators.[237] In the EU and the U.S.

[236] Mark Lemley et al, *Don't Break the Internet*, 64 STAN. L. REV. ONLINE 34, 35 (2011), http://www.stanfordlawreview.org/system/files/online/articles/64-SLRO-34_0.pdf.

[237] *Cf.*, Ethan Zuckerman, *Intermediary Censorship, in* ACCESS CONTROLLED: THE SHAPING OF POWER, RIGHTS, AND RULE IN CYBERSPACE 71 et seq. (Ronald Deibert et al. eds., 2010). *Cf. also Lukas Feiler, Beeinträchtigungen der Meinungsäußerungsfreiheit durch die Zensur des Internets in China und im Iran* [*Impairment of the Freedom of Expression by Internet Censorship in China and*

users have, until recently, not faced any such restrictions on the level of the Internet infrastructure.

The following chapters will examine the effects website blocking injunctions under Information Society Directive article 8(3) and Copyright Act § 512(j) will have on the aforementioned global infrastructure and the transatlantic market and will further discuss how these effects relate to the rule of national copyright law. First, Part 6.1 will describe how blocking injunctions may lead to a partitioning of the global Internet into multiple national Internets. Part 6.2 will then discuss the effects this technological fragmentation may have on the transatlantic market as well as the internal market of the EU. Part 6.3 will analyze the relationship between the rule of national copyright law and the fragmenting effects of blocking injunctions. Lastly, Part 6.4 will discuss the underlying conflict in the ongoing debate about website blocking injunctions.

6.1 The Partitioning of the Global Internet

As described *supra* in Part 6, the Internet's logical infrastructure has generally been a common resource shared without alteration across borders in different jurisdictions. A user entering a certain domain name or IP address could rely on that identifier being equally valid, irrespective of the jurisdiction she currently resided in. The possibility of website blocking injunctions somewhat alters this reality:

Whether and how one's Internet access provider resolves a domain name into an IP address is not anymore an exclusively technical question. From a user's perspective,

---

Iran], *in* NOTHING TO HIDE NOTHING TO FEAR?: DATENSCHUTZ – TRANSPARENZ – SOLIDARITÄT. JAHRBUCH MENSCHENRECHTE 2011 [NOTHING TO HIDE NOTHING TO FEAR?: DATA PROTECTION – TRANSPARENCY – SOLIDARITY. YEARBOOK HUMAN RIGHTS 2011] 269 et seq. (Heiner Bielefeldt et al. eds., 2011).

this means that responses that are provided by the Internet access provider's DNS server do not necessarily reflect the technical reality (i.e. how the domain's owner actually configured its domain).[238] More importantly, the responses that access providers deliver will depend on the jurisdiction in which the provider resides. Thus, a domain name like www.example.com might be resolved into the correct IP address when an Internet access provider in Germany is used and might be resolved into a non-routable IP address or not resolved at all when an Internet access provider in the U.S. is used. From a user's perspective the same domain name will thus correspond to different IP addresses, depending on the governing jurisdiction.

Once the new DNS Security Extensions (DNSSEC)[239] are more widely deployed, Internet access providers could indeed not, for a domain that is to be blocked, successfully respond with an incorrect IP address: DNSSEC requires all DNS responses to be signed with a cryptographic key that only the owner of the domain has access to.[240] Thus, the only way Internet access providers will then be able to

[238] Arguably, users should long have stopped trusting their Internet access providers to resolve domain names correctly. Many Internet access providers indeed resolve any non-existent domain into one of their own IP addresses that belongs to webservers that display a search engine along with paid-for advertisements. *See* ICANN SECURITY AND STABILITY ADVISORY COMMITTEE, PRELIMINARY REPORT ON DNS RESPONSE MODIFICATION, SAC 032 (2008), http://www.icann.org/en/committees/security/sac032.pdf.

[239] Specified in R. Arends et al., DNS Security Introduction and Requirements, RFC 4033 (2005), http://www.rfc-editor.org/rfc/rfc4033.txt; R. Arends et al., Resource Records for the DNS Security Extensions, RFC 4034 (2005), http://www.rfc-editor.org/rfc/rfc4034.txt; and R. Arends et al., Protocol Modifications for the DNS Security Extensions, RFC 4035 (2005), http://www.rfc-editor.org/rfc/rfc4035.txt.

[240] *Cf.* R. Arends et al., DNS Security Introduction and Requirements, RFC 4033, § 3 et seq. (2005), http://www.rfc-editor.org/rfc/rfc4033.txt. *Cf. also* T. Creighton et al., DNS Redirect Use by Service Providers, IETF Internet-Draft, § 4 (2010), http://tools.ietf.org/html/draft-livingood-dns-redirect-03 (stating that "[the] adoption of DNSSEC is technically incompatible with DNS redirect").

implement DNS blocking is by returning an error code instead of a valid response.[241] In this scenario, the same domain name will not be resolved to different IP addresses in different jurisdictions; rather, it will not be possible for users to tell whether the domain has been blocked or is currently affected by technical malfunction.

Similarly, with IP blocking in place, users will not anymore be able to use an IP address as a global identifier that functions irrespective of the jurisdiction their Internet access provider or Internet backbone provider resides in. If an IP address is blocked, the user's service provider will respond to a packet sent to that address with an error packet informing the user's computer that the destination is "unreachable."[242] Alternatively, the service provider may simply discard all packets addressed to a blocked IP address without sending any error response.[243] In any case, IP addresses would cease to be globally valid identifiers. Their validity would rather depend on the website blocking injunctions currently in force in the jurisdiction in question. Further complicating matters, an IP blocking injunction imposed on an Internet backbone operator is likely to also affect Internet access providers located in other countries than the backbone operator itself.

In summary, the possibility of website blocking injunctions results in a situation where the most fundamental identifiers on the Internet—IP addresses and domain

---

[241] *Cf.* Steve Crocker et al., Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill 6 (2011), http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf.

[242] Such Destination Unreachable Message are sent using the Internet Control Message Protocol. *See* J. POSTEL, INTERNET CONTROL MESSAGE PROTOCOL, RFC 792, at 3 (1981), http://www.rfc-editor.org/rfc/rfc792.txt.

[243] *See* BARRY RAVEENDRAN GREENE, REMOTE TRIGGERING BLACK HOLE FILTERING—ISP ESSENTIALS SUPPLEMENT 2 (2002), ftp://ftp-eng.cisco.com/cons/isp/essentials/Remote%20Triggered%20Black%20Hole%20Filtering-02.pdf.

names—will not anymore be equally valid anywhere on the Internet. Rather, users in each jurisdiction will have a somewhat different perspective of the Internet as valid IP addresses and domain names will be different for each jurisdiction. Ultimately this leads to a partitioning of the global Internet into multiple national Internets.

The question of whether the partitioning of the Internet into Nation-Nets is necessarily a negative development is often answered quickly with reference to technical principles like "domain name universality."[244] However, not only have such technical principles already been watered down in practice;[245] more importantly, compliance with a technological principle does not, in and of itself, have any inherent public policy value. The following chapter will therefore examine the potential effects of website blocking injunctions from an economic perspective

6.2 Market Fragmentation

The Internet's global infrastructure has undoubtedly been a significant contributing factor to the formation of a transatlantic market covering the U.S. and the EU. Indeed, any website that went online in the U.S. was necessarily also available in the EU, making the U.S. and all of the EU's Member States often function as a single market for online services. Similarly, the internal market of the EU also greatly benefited from the Internet.

Recognizing the importance of the Internet for the internal market of the EU, the EU legislature specifically adopted the E-Commerce Directive in particular "to avoid

[244] Mark Lemley et al, *Don't Break the Internet*, 64 STAN. L. REV. ONLINE 34, 35 (2011), http://www.stanfordlawreview.org/system/files/online/articles/64-SLRO-34_0.pdf.

[245] *See supra* note 238.

fragmentation of the internal market."[246] It is with this aim that E-Commerce Directive article 3(2) generally prohibits Member States from restricting the freedom to provide information society services from another Member State as long as they comply with the laws of their Member State of establishment (origin principle).[247]

However, as mentioned *supra* in Part 5.2, this prohibition does not apply to those areas of the law that are referred to in the annex of the E-Commerce Directive.[248] Significantly, this also includes copyright.[249] It is thus apparent that the drafters of the E-Commerce Directive have recognized the risk that differing national copyright laws pose for the common internal market but have nonetheless decided to accept that risk.

The wording of IPRED article 3(2) also makes clear that the risk of market fragmentation has been recognized. The provision states that the measures, procedures and remedies necessary to ensure the enforcement of the intellectual property rights "shall be applied in such a manner as to avoid the creation of barriers to legitimate trade."[250] However, what constitutes "legitimate" trade is, of course, again to be determined by the copyright law of each Member State.[251] Thus, the

[246] E-Commerce Directive recital 59.

[247] *Cf. supra* Part 5.2.

[248] *See* E-Commerce Directive art. 3(3).

[249] *See* E-Commerce Directive annex, first indent.

[250] IPRED art. 3(2).

[251] Assuming of course that the law of the Member State in question is in compliance with EU law, e.g. the Information Society Directive.

requirement that injunctions should not create barriers to legitimate trade has only limited practical effect.[252]

Article 41(1) of the TRIPS Agreement[253] also provides that intellectual property rights enforcement procedures "shall be applied in such a manner as to avoid the creation of barriers to legitimate trade."[254] The same wording is also contained in Article 6(1) of the Anti-Counterfeiting Trade Agreement (ACTA)[255] which has not yet entered into force.[256]

For both treaties, it has to be noted that a trade in digital goods or services that violate national copyright law that was adopted pursuant to and in compliance with the treaties cannot be considered "legitimate" trade.[257] Thus, generally speaking,

---

[252] *Cf.* Michel Walter & Dominik Goebel, *Enforcement Directive*, *in* EUROPEAN COPYRIGHT LAW: A COMMENTARY 1193, 1224 (Michel Walter & Silke von Lewinski eds., 2010) (noting that this requirement "must not be overrated").

[253] Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, 33 I.L.M. 1125 (1994).

[254] TRIPS Agreement art. 41(1). *Cf.* DANIEL GERVAIS, THE TRIPS AGREEMENT: DRAFTING HISTORY AND ANALYSIS 441 (2008) (noting that "[t]he need for effectiveness must also take account of the need to avoid the creation of barriers to legitimate trade").

[255] Anti-Counterfeiting Trade Agreement, Oct. 1, 2011, *available at* http://www.mofa.go.jp/policy/economy/i_property/pdfs/acta1105_en.pdf. *Cf. also id.* art. 27(2) (stating particularly with regard to enforcement in the digital environment that enforcement procedures "shall be implemented in a manner that avoids the creation of barriers to legitimate activity").

[256] ACTA will not enter into force before at least six signatory states have ratified it. *See ACTA* art. 40(1). At the time of this writing, no such ratifications were yet performed. *See* http://ec.europa.eu/trade/creating-opportunities/trade-topics/intellectual-property/anti-counterfeiting/#timeline (last accessed Feb. 15, 2012).

[257] *Cf.* Henning Grosse Ruse-Khan, *A Trade Agreement Creating Barriers to International Trade?: Acta Border Measures and Goods in Transit*, 26 AM. U. INT'L L. REV. 645, 700 (2011) (noting that "the operation of the prohibition to create barriers to legitimate trade cannot be understood in a way which prohibits [measures] that ACTA explicitly allows or even mandates").

Article 41(1) of the TRIPS Agreement does not and ACTA will not pose an obstacle for website blocking injunctions based on copyright infringement.

6.3 The Rule of National Law and Its Necessarily Fragmenting Effect

Since the origin principle of the E-Commerce Directive does not apply in the area of copyright law,[258] every Member State has to apply its own copyright law to a website that is available in its jurisdiction. Similarly, when a website of an EU company is available in the U.S., U.S. courts have to look to U.S. copyright law to determine the legality of the website's content.

The parallel application of national copyright laws is indeed a reasonable result because each country has a legitimate interest to enforce its own laws. This, of course, also applies to other areas of the law such as anti-trust law or defamation law. For example, the merger between NYSE Euronext which operates, *inter alia*, the New York Stock Exchange, and Deutsche Börse which operates, *inter alia*, the Frankfurt Stock Exchange, was approved by the U.S. Justice Department in December 2011[259] but vetoed by the European Commission in February 2012.[260] In *Dow Jones & Co. Inc. v. Gutnick*,[261] the High Court of Australia found that Dow Jones, the U.S.-based publisher of a newspaper that was also available online in Australia was liable for defamation, based on Australian defamation law, noting that

[258] *See supra* Part 5.2.

[259] *See* Michael J. del la Merced, *Justice Dept. Approves Merger of NYSE Euronext and Deutsche Borse*, NYTIMES.COM, Dec. 22, 2011, http://dealbook.nytimes.com/2011/12/22/justice-approves-merger-of-nyse-euronext-and-deutsche-borse/?ref=nyseeuronext.

[260] *See* Press Release, European Commission, Mergers: Commission blocks proposed merger between Deutsche Börse and NYSE Euronext (Feb. 1, 2012), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/94.

[261] Dow Jones & Co. Inc. v. Gutnick (2002) 210 C.L.R. 575 (Australia).

"[t]he fact that publication might occur everywhere does not mean that it occurs nowhere."[262] Similarly, in *Ligue Contre le Racisme et l'Antisémitisme v. Yahoo! Inc.*, the Tribunal de Grande Instance of Paris found Yahoo! liable for violating French law that prohibits the sale or auctioning of Nazi memorabilia.[263]

These cases illustrate that trans-border activities are subject to the laws of both countries involved. To the extent that these laws differ, there will necessarily be additional barriers to trade and thus a certain extent of market fragmentation. In the cases above, the laws of all relevant jurisdictions have to be respected to carry out the activity in question: NYSE Euronext and Deutsche Börse may only merge if approved by U.S. and EU authorities; a website that is available in multiple jurisdictions (and also has seizable assets there) should violate none of the jurisdictions' defamation laws; and an internationally active auction website should only sell those goods that are legal in its own, the seller's, and the buyer's jurisdiction. Thus, in the above examples, the lowest common denominator of what is permissible under the applicable national laws is the relevant standard for a corporation. This increases compliance costs for internationally active companies, thereby (necessarily) creating new barriers to trade.

Website blocking injunctions are a means of enforcing one country's copyright law against foreign websites. They are, thus, also an example of subjecting the same activity—making a website publicly available—to multiple jurisdictions. However, they differ from the examples above in one important respect: They are a means of enforcing the law through local intermediaries (Internet access providers and

[262] *Id.* at § 186.

[263] Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, Nov. 20, 2000 (Fr.), *available at* http://juriscom.net/documents/tgiparis20001120.pdf.

Internet backbone operators) as opposed to a means of enforcing the law at the source of the infringement.[264] This has two implications that are highly relevant here:

First, website blocking injunctions have a stronger market-fragmenting effect. In the examples above, the laws of different jurisdictions are enforced against the source of the infringement which is thus forced to comply with all of the requirements. Since it will typically do so, this will only increase the costs of compliance (e.g. with U.S. anti-trust law and EU competition law) but will, by the operation of the law itself, not necessarily result in a situation where a company offers differing goods and services depending on the jurisdiction.

By comparison, website blocking injunctions automatically bar the blocked website from entry into the local market while still allowing the website to be available in other geographic markets. Thus, website blocking injunctions—by their very nature as means of enforcement through local intermediaries—necessarily lead to a more direct and typically much stronger market fragmentation than enforcement measures directed against the source of an infringement.

There is a second implication of the fact that website blocking injunctions are enforced against local intermediaries. These injunctions have a much more limited extraterritorial effect as they only prevent residents of the country where the injunction is issued from accessing the foreign website. They do not prevent the foreign website from making its content available to other jurisdictions and do not impose a fine on the website's operator.

[264] *Cf.* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET 69 et seq. (2006) (discussing how government rule the net by exerting extraterritorial control through local intermediaries).

In summary, website blocking injunctions have, when compared to enforcement measures directed towards the source of the infringement, only a limited extraterritorial effect. They do, however, lead to a more direct and typically stronger market fragmentation. What has to be kept in mind is that when the foreign source of the infringement has no seizable assets within the jurisdiction's reach, a website blocking injunction is often the only way applicable copyright law can be enforced.

Thus, if the rule of applicable (national) copyright law is to be enforced, website blocking injunctions seem to be a necessity. From this perspective, the root cause of the market-fragmenting effect of website blocking injunctions is that national copyright laws differ and will therefore prohibit the provision of certain services in one country while allowing them in another. It is therefore not the way in which copyright law is enforced—in particular by website blocking injunctions—but rather copyright law itself, or more precisely, the fact that national copyright laws differ from one another that ultimately leads to a fragmentation of the global Internet and the transatlantic market.

6.4 The Rule of Copyright Law and Why a Debate about Enforcement of the Law is a Bad Substitute for a Debate about the Law Itself

The claim that the Internet existed in a legal vacuum[265] has long been rebutted.[266] Thus, people generally have little doubt that the law regulates online activities the same as offline activities. Most members of society would also agree that they benefit from this rule of law over the Internet—whether in the area of e-commerce law, data privacy, or anti-trust law.

[265] *Cf., e.g.*, John Perry Barlow, A Declaration of the Independence of Cyberspace, Feb. 8, 1996, https://projects.eff.org/~barlow/Declaration-Final.html.

[266] *Cf., e.g.*, Lawrence Lessig, Code and Other Laws of Cyberspace 24 (1999).

The debate about website blocking injunctions is essentially a debate about whether to subject to the rule of national copyright law content that is made available on foreign websites. Why then is there such a strong opposition against the rule of copyright law over foreign content, given that the rule of law over the Internet itself has long been accepted?

The most plausible answer is that many people do not see copyright law as benefiting them and their interests. This is, however, not the subject of the current debate in the EU or the U.S. Indeed, the scholarly debate as well as the public debate is focused on whether to enforce copyright law and fails to address the more fundamental question of whether substantive copyright law itself is actually representative of the—often conflicting—interests of all stakeholders.

The current enforcement debate is necessarily reduced to a question of all or nothing—to enforce all of copyright law against foreign websites or to effectively exempt foreign websites entirely from the reach of copyright law. In this debate, all nuances are lost: While one side claims that without website blocking injunctions, the entire copyright system would ultimately fail,[267] the other side claims that blocking injunctions would destroy the Internet as we know it.[268] A debate between such extreme positions—all or nothing—is unlikely to be productive and, more importantly, will prevent any discussion about the actual reasons why many people

[267] *Cf. Hearing on H.R. 3261, the "Stop Online Privacy Act" Before the House Comm. on the Judiciary*, 112th Cong. (2011) (statement of Maria A. Pallante, Register of Copyrights), *available at* http://www.copyright.gov/docs/regstat111611.html (stating that "if Congress does not continue to provide serious responses to online piracy, the U.S. copyright system will ultimately fail […]. SOPA is the next step in ensuring that our law keeps pace with infringers").

[268] *Cf., e.g.*, Mark Lemley et al, *Don't Break the Internet*, 64 STAN. L. REV. ONLINE 34 (2011) http://www.stanfordlawreview.org/system/files/online/articles/64-SLRO-34_0.pdf.

see substantive copyright law as detrimental to their interests and thus do not want it to be enforced.

For example, should the copyright term indeed be the life of the author plus 70 years even though all but very few copyrighted works lose their commercial value within a few years?[269] Should the exceptions from copyright (in particular the fair use doctrine under U.S. copyright law) be construed as narrowly as they currently are? Should the law provide statutory damages of up to $150,000 as Copyright Act § 504(c)(2) currently does in the case of willful infringement?

More generally, most questions of substantive copyright law can also be seen as a question of the proper balance between the freedom of expression and the freedom of information on one side and copyright on the other. Indeed, it seems that this question is at the core of the discontent many people have for copyright law as it stands today: Nearly all of our online activities either consist in expressing ourselves or obtaining information that seems valuable to us—whether we post a video on YouTube showing a family member dancing to a popular song, download an episode of a critically acclaimed TV series that will never be broadcast in one's country, or use pictures of comic characters as profile pictures on Facebook. All of this speech is tightly regulated by copyright law.

Whether and to what extent it also should be, is a discussion worth having. Since copyright law regulates more or less everything we do online, scholarly research as well as the public in general should re-engage in a debate about the substance of

[269] *See* Lawrence Lessig, Free Culture: The Nature and Future of Creativity 221 (2004); *cf. also* Lawrence Lessig, The Future of Ideas: The Fate of the Commons in a Connected World 251 (2001) (arguing for a drastic reduction of the copyright term).

copyright law itself and, in particular, how we should weigh copyright against the freedom of expression and the freedom of information.

7. Conclusion

The recent debate over SOPA and PIPA has brought the issue of website blocking to the forefront of public debate. However, it is often neglected that U.S. as well as EU copyright law already provide for the possibility of website blocking injunctions. While only a single case has been reported from the U.S., there are already eight cases in which courts of EU Member States have imposed such blocking injunctions.

Website blocking injunctions will, to some degree, lead to a partitioning of the global Internet and will also have a market-fragmenting effect. However, this is an inevitable result of the rule of national law over the Internet since the applicable laws differ from one country to another and are also not always enforced to the same extent.

The current debate over website blocking injunctions or, more generally, the enforcement of copyright law, is certainly an important one. However, to address the underlying reasons why many people oppose the enforcement of copyright law in this context, a more fundamental discussion is needed. It should address the substance of the law and in particular the proper balance between the freedom of expression and the freedom of information on one side and copyright on the other.