COORDINADORES
Joan Balcells Padullés
Agustí Cerrillo i Martínez
Miquel Peguera Poch
Ismael Peña López
María José Pifarré de Moner
Mònica Vilasau Solana

Internet, Derecho y Política
Una década de transformaciones

Actas del X Congreso Internacional Internet, Derecho y Política.
Universitat Oberta de Catalunya, Barcelona, 3-4 de julio de 2014

Internet, Law & Politics
A Decade of Transformations

Proceedings of the 10th International Conference on Internet, Law & Politics.
Universitat Oberta de Catalunya, Barcelona, 3-4 July, 2014

UOC
Universitat Oberta de Catalunya
HUYGENS EDITORIAL

WEBSITE BLOCKING: EVOLUTION OR REVOLUTION? 10 YEARS OF COPYRIGHT ENFORCEMENT BY PRIVATE THIRD PARTIES

Ellen Marja Wesselingh
The Hague University of Applied Sciences

ABSTRACT: Copyright enforcement by private third parties –does it work uniformly across the EU? Since the inception of Napster, home copying of digital files has taken a flight. The first providers of software or infrastructure for the illegal exchange of files were held contributory or vicariously liable for copyright infringement. In response, they quickly diluted the chain of liability to such an extent that neither the software producers, nor the service providers could be held liable. Moving further down the communication chain, the rights holders are now requiring Internet Service Providers (ISPs) that provide access to end customers to help them with the enforcement of their rights. This article discusses case-law regarding the enforcement of copyright by Internet Access Providers throughout Europe. At first glance, copyright enforcement has been harmonised by means of a number of directives, and article 8(3) of the Copyright Directive (2001/29/EC) regulates that EU Member States must ensure the position of rights holders with regard to injunctions against ISPs. Problem solved? Case law from Denmark, Ireland, Belgium, Norway, England, The Netherlands, Austria and the Court of Justice of the EU was studied. In addition, the legal practice in Germany was examined. The period of time covered by case law is from 2003 to 2013, the case law gives insight into the differences that still exist after the implementation of the directive.

KEYWORDS: Copyright, enforcement, case law, EU, intermediary service providers.

1. INTRODUCTION

In the past twenty years, the media landscape has changed drastically. The dissemination of creative works of any kind used to be controlled by professional parties. Consumers were consuming media, the re-use of existing media –for example playing songs in a theatre– was regulated with licenses and neighbouring rights. This has changed. Transaction and distribution costs have gone down due to the availability of digital media, making it possible for consumers to become producers and distributors of materials. These new opportunities for sharing have both good and bad effects. A positive effect can be found in some scientific communities where Open Access is slowly becoming the norm. A negative effect can be found in the peer-to-peer (P2P) file sharing facilitated by entities like The Pirate Bay. This new «norm» of sharing has created friction with the old system of copyright protection.

In the beginning of the twenty-first century, P2P file sharing was enabled in a more or less centralised way; most well-known is probably the Napster case (A&M Records v Napster, 2001). The company Napster was consequently held legally responsible for copyright infringement: by allowing users to infringe copyright directly, Napster committed contributory (§48-49) and vicarious copyright infringement (§60). Essential elements were that Napster provided the software for the user, maintained on its own servers search index software that enabled the connection and provided a hotlist of users of interest also currently logged on to the Napster server (§10-11). The court did not rule the mere existence of the Napster system as a ground for contributory and vicarious liability (§84-85).

The Napster case inspired other software developers to build different systems, with less centralised indexes. This decentralisation eventually led to the model used by The Pirate Bay. This website started in 2003 and has grown to one of the largest file sharing facilitators (website The Pirate Bay, 2014). The website started as a Bittorrent tracker; a list of so-called torrents that identify which file can be found where (Pouwelse, Garbacki, Epema & Sips 2005). The torrent files do not contain copyrighted materials themselves; they provide access information on where the material files can be found on the network. Rights holders successfully sued The Pirate Bay for (complicity in) copyright infringement in the EU Member States Sweden and The Netherlands (Sony Music Entertainment et al v Neij et al, 2009, B 13301-06) (Brein v The Pirate Bay, 2009, 428212-KG ZA 09-1092). As a result, The Pirate Bay switched to the provision of Magnet Links, files that do not point to an address on the network but to a cryptographic hash value that indicates the content of the file. This so-called Distributed Hash Table (DHT) technology was built to circumvent legal action by rights holders (Wolchok & Halderman, 2010, chapter 2).

By switching to this new technique, the operators of the P2P file sharing website no longer have any knowledge of the exact content of the files that the cryptographic hash value refers to, where companies like Napster and Grokster did have actual knowledge. Because the Internet has been mostly borderless in the past years, it has been very difficult for the nationally organised legal systems to enforce the shutdown of websites facilitating P2P file sharing. When being targeted with legal action, the operators simply move their business to another jurisdiction and the whole process of shutting down the business by court order starts from scratch in the new jurisdiction. As a result, the rights holders have moved down the chain of communication, away from the service suppliers of a specific P2P file sharing service towards the supplier serving the end customer Internet access. When we look at a model of communication, this process can be depicted as shown in figure 1.

The next sections discuss that process. This article uses the terminology Internet Service Provider (ISP), which encompasses all types of services, including providing end customers with Internet access, in which case the ISP will be named Internet Access Provider.

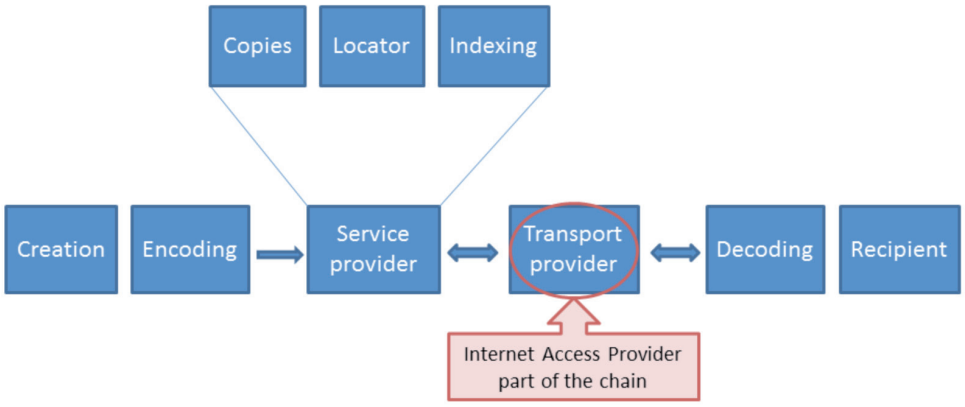


Figure 1: a model of transport of information. The model is based on the models of Shannon-Weaver Mathematical Model (1949) and Schramm's Model of Communication (1954) (see annex). Creation: the conceptualisation of a creative idea. Encoding: deciding in which format to publish the creative idea: print, sound, visual, et cetera. The "Service provider" is the provider of the platform that enables P2P exchange. The Internet Access Provider is one of the Transport providers (the provider enabling access to the recipient in this figure). It must be noted that noise can be added in any stage of the process.

2. HARMONISATION OF COPYRIGHT ENFORCEMENT IN THE EU

The original maxim was to enforce copyright (and related rights) at the source. Rights holders would sue the service provider (operator of the website containing the infringing materials or linking to infringing materials), such as in the Napster case.[1] Even Grokster, which had decentralised the business to avoid liability, was still held liable because it actively promoted copyright infringement by use of its service (Ricketson & Ginsburg, 2006). As discussed above, this model no longer works due to the ease with which service providers can move their business to another jurisdiction. The rights holders that wanted to enforce their copyrights had a few other options: either suing the end user, or forcing the end users' («mere conduit») internet access providers to block the infringing website. The latter is what most copyrights owners' representatives throughout the EU do.

At a first glance, in the European Union the enforcement of copyright has been harmonised in the Information Society Directive (2000/31/EC), the Copyright Directive (2001/29/EC) and the Copyright enforcement Directive (2004/48/EC). The Euro-

1 Many cases followed: Grokster/Kazaa, E-donkey, Limewire, FTD, Mininova, Newzbin, Kino to name just a few.

pean Union strives towards a single market and encourages the establishment of a level playing field in the telecommunications sector because that would form the foundation of said single market. The single market offers opportunities to legal business as well as illegal business, and the EU would like to encourage legal business while at the same time fight the infringement of rights of those doing legal business. Preamble section 59 and article 8 of the Copyright Directive are a reflection of the recognition that the services of intermediaries may be used for infringing rights of others in the digital world.

Section 59 of the preamble of Copyright Directive 2001/29/EC states: «*In the digital environment [..] services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries* [Internet Access Providers] *are best placed to bring such infringing activities to an end*. [..] *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*. [..] *The conditions and modalities relating to such injunctions should be left to the national law of the Member States*.» and article 8 states: «[..] *3. Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right*.» There is some harmonisation, but the exact implementation of the instrument of injunction is left to the Member States.

3. BLOCKING OF COPYRIGHT INFRINGING WEB SITES BY THIRD PARTIES

In Spain, rights holders have tried to bring to court individual end customers in an effort to stop copyright infringement. Rights holders' representative Promusicae sued ISP Telefónica for the personal details of customers behind IP addresses that were found to engage in P2P file sharing, in 2005. In January 2008 the European Court of Justice found that the directives regarding copyright do not require Member States to oblige the communication of personal data in civil proceedings, but that the Member States may implement such measures in accordance with Community law, such as the principle of proportionality (Promusicae v Telefónica). Similar proceedings happened in Ireland in 2005 ([2005] IEHC 233). However, turning to individual end customers has not become mainstream practice in Europe, the rights holders have mostly turned to ISPs to block the content rather than bringing individual citizens to court. In this section case law from various European countries regarding the blocking of P2P facilitating websites is discussed in a more or less chronological order.

3.1. Denmark: the early years

The first cases in Denmark were directed at Internet Access Providers to identify FTP (File Transfer Protocol) service providers serving copyright infringing materials

from their servers. In several court cases from 2003 to 2006 (TDC Totalløsninger v IFPI), the Internet Access Providers were ordered to provide the contact details of the FTP operators. From 2006 onward, P2P file sharing service providers were targeted by rights holders. Because these service providers operated abroad, the Danish Internet Access Providers were ordered to block the websites. The case of the rights holders (represented by IFPI Denmark) against Tele 2 A/S was decided in the first instance on 25 October 2006 (Aller International v Tele2). The court ordered Tele2 to block the website www.allofmp3.com, followed by a second decision in which Tele2 was ordered to block www.mp3sparks.com on 15 August 2007.

The case IFPI Denmark v DMT2 A/S was decided in the first instance on February 5th 2008 (Bailiff's Court of Frederiksberg). The court ordered the blocking of the website www.thepiratebay.org and its subpages and subdomains, without further specification of the technical measures to be implemented by the Internet Access Provider to comply with the order. The blocking order was appealed by the provider (High Court, 26 November 2008) and finally decided on May 27, 2010 by the Supreme Court (UfR 2010:2221-2230). In the first instance, no specific technical measures were considered; the court sufficed with a general order for the Internet Access Provider to take the necessary measures to prevent access. On appeal, four specific measures were considered: hardware or software content filtering (Deep Packet Inspection or DPI),[2] installing a proxy,[3] blocking DNS traffic,[4] and blocking IP addresses.[5] The same court already considered these four measures in an appeal case of 2 August 2006.[6]

Of these four options, the Supreme Court only considered DNS blocking a viable option. DPI is considered to be too expensive for Internet Access Providers, both economically and in data traffic delay. The proxy solution is troublesome with encrypted (HTTPS) traffic, which is frequently used in Virtual Private Networks (VPNs). IP-addresses often change frequently and may host more websites than just the infringing site, and apart from these issues IP addresses were considered to be personal data in the earlier judgements regarding FTP-server operators. The drawback of DNS blocking, that it can be easily circumvented, is not considered to be a problem, the courts are of the opinion that «*Blocking at the DNS-level are generally sufficiently effective*» (Sonofon v IFPI Danmark). The Internet Access Providers claimed «*the prohibition and injunction is*

2 UfR 2010:2224. «Metode 1: Installation af hardware og software mellem ISP'ens internetforbindelse og deres kunders adgang.» The specific technology mentioned is Content Filtering by Sonicwall.

3 UfR 2010:2224. «Metode 2:Etablering af en såkald Proxy.»

4 UfR 2010:2225.

5 UfR 2010:2225.

6 UfR 2010:2229.

not sufficiently clear and precise, not proportional and subsidiary»[7] but the Supreme Court disagreed and upheld the order to block The Pirate Bay website with the use of DNS-blocking.[8]

Preventing access to websites by Internet Access Providers using DNS-blocking is considered a solution in Denmark. In January 2013, six websites were blocked by all Internet Access Providers in Denmark for enabling the illegal exchange of copyrighted materials. The list is growing; in October 2013 a total of 10 websites were listed.[9]

3.2. Belgium: the first references to the CJEU

In Belgium, blocking of websites by Internet Access Providers was also the subject of discussion in court cases. The Belgian court of first instance discussed in detail what type of technology the Internet Access Provider may use to implement the blocking order: a network appliance using Deep Packet Inspection (Hughes, Mady & Bourrouilhou 2007). However, the blocking order by the court was of a more general nature, stating that the Internet Access Provider shall stop copyright infringements by disabling file sharing through P2P, without giving technical specifications.

The Belgian appeal court found reasons to ask prejudicial questions regarding the issuance of a blanket order upon an Internet Access Provider to install a filtering system for all its' customers to the Court of Justice of the EU in Luxembourg (Scarlet v Sabam). In answering the prejudicial questions, the Court of Justice of the EU found that no Deep Packet Inspection shall be ordered in this type of case. The Court defined the steps that a DPI system performs (Scarlet v Sabam, 24 November 2011):

1. To identify within all of the electronic communications the peer-to-peer traffic;
2. Identify with the peer-to-peer traffic files containing works that may be subject to a copyright claim;
3. Determine which files are actually being shared unlawfully;
4. Preventing the availability of these files that contain works subject to a copyright claim.

The Sabam v Netlog case (16 February 2012) concerned a social network instead of an Internet Access Provider. However, the Court concluded similar: no service pro-

7 UfR 2010:2229.

8 UfR 2010:2230.

9 Tele Industrien provides a list (http://www.teleindu.dk/brancheholdninger/blokeringer-pa-net-tet/), in January 2013 the following websites were listed: www.allofmp3.com (2006/7), www.mp3sparks.com (2006/7), www.thepiratebay.org (2008), www.thepiratebay.se (2012), www.homelifespain.com (2012), and www.grooveshark.com (2012). www.dreamfilm.se, www.swefilmer.com, www.primewire.ag and www.movie4k.to were added in October 2013.

vider can be required to implement a general monitoring obligation that is unlimited in time, monitors all users without prejudice for an unlimited period of time and must be funded exclusively at the cost of the service provider. This is in line with previous case law concerning a service provider enabling the online trade of physical goods (L'Oréal v Ebay). In this case service providers may be required to block activities involving trademark infringement (including future infringements), but there can be no general monitoring obligation. According to the Court, the prohibition of a general filtering obligation under preamble sub 47 and article 15(1) of the Information Society Directive (2000/31/EC) is applicable to Internet Access Providers (Scarlet v Sabam) as well as Social Networks as hosting providers (Sabam v Netlog).

In both the Scarlet v Sabam and Sabam v Netlog cases the Court considered the human rights as defined in the Charter of Fundamental Rights of the EU, most notably the freedom to do business (Scarlet §46, Netlog §44), privacy of individual customers (Scarlet §51, Netlog §48-49) and freedom of expression (Scarlet §52, Netlog §50). The material questions on whether one right or the other must prevail in a specific case must be left to the national court, especially since statutory exceptions to copyright exist among EU Member States (Scarlet §52, Netlog §50).

3.3. The United Kingdom: a shift in technologies prescribed

In the UK, a number of cases went all the way to the High Court. After unsuccessfully ordering the website Newzbin to close down in 2010, the court ordered Internet Access Provider British Telecom (BT) to block the website Newzbin2 in July 2011 (Fox v BT, [2011] EWHC 1981). In April 2012, providers Sky, BT, Everything Everywhere, TalkTalk, Virgin Media and Telefónica were ordered to block The Pirate Bay (Dramatico v B Sky B, [2012] EWHC 268). In February 2013, the same providers were ordered to block the websites KAT (Kickass Torrents), H33T and Fenopy (EMI v B Sky B, [2013] EWHC 379). Without being exhaustive, the list shows that blocking is a popular method.

Based on section 97A CDPA 1988, which implements article 8(3) of the Copyright Directive,[10] the rights holders wanted that «*The Defendant* [access provider British Telecom] *shall prevent its services being used by users and operators of the website known as NEWZBIN and NEWZBIN2 to infringe copyright.*»[11] Regarding the technology to be implemented, the revised request was that «*The Respondent* [British Telecom] *shall adopt the following technology directed to the website known as Newzbin or Newzbin2 currently accessible at www.newzbin.com and its domains and sub domains. The technology to be adopted is:*

10 Fox v BT §153 & §158.

11 Fox v BT §11.

(i) *IP address blocking in respect of each and every IP address from which the said website operates or is available* [..].

(ii) *DPI based blocking utilizing at least summary analysis in respect of each and every URL available at the said website and its domains and sub domains* […].»[12]

We see that the High Court orders Deep Packet Inspection, and specifies in detail that all web addresses (Uniform Resource Locators or URLs) of all websites that are being visited by all the BT customers must be checked, in order to find the main domains and the subdomains operated by Newzbin, and subsequently filter out these domains. In the final order given, it was reiterated what type of technology the Internet Access Provider shall use to implement the blocking order.[13] The reasoning in the Newzbin case shows that the Court did consider the issues of and freedom of expression (§76-77, 164) and the right to property (§78). Privacy was not explicitly considered, reference was made to the Privacy directive 95/46/EC (§79 and 88) and to case law of the European Court of Justice (§155). The issue of freedom of doing business was not considered by the Court in its weighing of rights.

Nearly a month after the Newzbin case, the Court of Justice of the EU delivered its interpretation of the EU law in the Scarlet v Sabam case on 24 November 2011. This judgement clearly prohibited courts under EU law to order blocking of websites with the use of DPI techniques. From then on, the High Court issued blocking orders by application of different techniques:

«[…] The technology to be adopted is:

(i) IP blocking in respect of each and every IP address from which the said website operates and which is:

(a) notified in writing to the Respondent by the Applicants or their agents; and

(b) in respect of which the Applicants or their agents notify the Respondent that the server with the notified IP address blocking does not also host a site that is not part of the Newzbin2 website.

(ii) IP address re-routing in respect of all IP addresses that provides access to each and every URL available from the said website and its domains and sub-domains and which URL is notified in writing to the Respondent by the Applicants or their agents; and

(iii) URL blocking in respect of each and every URL available from the said website and its domains and sub-domains and which is notified in writing to the Respondent by the Applicants or their agents.» (Dramatico v Sky, 2012).

12 Fox v BT §12.

13 Fox v BT Order, issued 26 October 2011.

At the time of this writing, many websites in the United Kingdom are blocked (well-known examples are www.newzbin.com and www.thepiratebay.org), but due to the various methods used by ISPs it remains uncertain how many websites exactly are blocked. However, the list contains at least 150 named websites that are being blocked according to an activist collection page (Immunicity, 2014).

3.4. Austria: not too specific, are generic blocking orders the answer?

In Austria, article 8(3) of the Copyright Directive is implemented in §81 of the federal law regarding the copyright on works of literature and art and concerning neighbouring rights.[14] Court judgements are phrased in two stages: first, a blocking order is given to an Internet Access Provider, ordering the provider to take whatever measures are necessary to block a website without specifying in detail when and technically how the website(s) shall be blocked by the access provider. This issue creates legal uncertainty («*Rechtsunsicherheit*») of subjects regarding the application of the law in a certain case: an Internet Access Provider is not really capable to judge the validity of a blocking request by a private party, especially regarding the requirements of «systematic» and «regular» infringement as argued in court cases. The technical measures taken by the provider must be tested by an independent judge upon request of rights holders. A ban («*Erfolgsverbot*») and independent judgement are not necessary mutually exclusive in the opinion of the Austrian government (Wesselingh, 2013).

The Austrian High Court asked prejudicial questions about the procedure to the European Court of Justice (UPC Telekabel Wien, 2012, C-314/12). The questions referred to by the Austrian High Court ask whether the website illegally providing copyright protected material is using Internet Access Provider services when customers of that access provider download copyrighted content, and if downloading for private use from an illegal source is permitted if providers of illegal material are not using the services of the access providers mentioned in the first question. The third prejudicial question asked whether a blocking order without specific technical implementation is considered compatible with EU Law, the final question concerned whether the cost of implementation would be a prohibiting factor for a blocking order.

In November 2013, the Advocate General issued his opinion on these questions, the judgement of the Court followed on 27 March 2014. A website illegally providing copyright protected material is using the services of an Internet Access Provider whose customers access that copyright protected material (Advocate General §59, Court §40). According to the Advocate General, a so-called «*Erfolgsverbot*» (a generically formulated blocking order for a specific website) that is being ordered upon a third party that does

14 Bundesgesetz über das Urheberrecht an Werken der Literatur und Kunst und über verwandte Schutzrechte.

not have a contractual relationship with the infringer, is contrary to the requirements as set in article 8(3) of Copyright Directive 2001/29 (§71), not providing a fair balance between enforcement of copyright and freedom of expression (§82) and freedom of enterprise (§83). The Court did not find that EU law precludes this *Erfolgsverbot*, provided it does not hinder lawful information access and the measure is effective in preventing unlawful access(§64).

There are some potential issues with a generically formulated order without specification of the technical measures to be implemented by a third party to stop copyright infringement, notably the legal insecurity. However, given the fact that case law of the CJEU shows unequivocally that very specific and targeted solutions such as Deep Packet Inspection are not allowed, and there is a right to freedom of enterprise, a more generic blocking order which allows the third party to make choices of implementation seems an appropriate solution.

3.5. Norway and The Netherlands: no, yes, err... no (or maybe yes)

In most countries discussed before, the reasoning and exact implementation of the solution to copyright infringement via P2P networks is not similar in detail, but the outcome at the highest level of abstraction is similar: a website shall be blocked by the Internet Access Provider. In some countries the order is accompanied by detailed technical implementation requirements whereas in other countries the implementation is left to the access provider. However, there are even some exceptions to the blocking orders issued.

In 2010, the Norwegian Court of Appeals refused an interim measure in the application for a preliminary injunction by various rights holders. The rights holders had sought an order requiring an Internet Access Provider to cease contributing to infringements committed through the P2P exchange site The Pirate Bay. The Court of Appeals confirmed the rejection by the Court of first instance and refused the requested measure, since article 8(3) of the Copyright Directive was not specifically implemented in Norwegian law (Nordic Records v Telenor, 2010).[15] The Court noted that despite the fact that the dispute had been going on for several years, the rights holders had not started substantive proceedings to order Telenor to block The Pirate Bay (p. 22), indicating that the Appeals Court did not find an urgent reason for an interim measure.

In one Dutch case in summary proceedings, the court dismissed a blocking order sought in 2010 (Brein v UPC, 2010). The request for a blocking order was rejected based on proportionality (a minority of customers is infringing but the order concerns all customers), no concrete individualised infringement, not clear why it would not

15 Although Norway is not a party in the EU treaties, in practice it does follow EU law.

be possible to call to justice one or more individuals, and no individual users could be heard in court. Subsequent substantive proceedings before the court in The Hague in first instance, led to blocking orders imposed on all major Internet Access providers in 2012 (Brein v Ziggo, 2012) (Brein v UPC, 2012).

In appeal, the Court of Appeals in The Hague ruled in January 2014. The providers Ziggo and Xs4all had appealed the order imposed on them to block the websites of The Pirate Bay (TPB) in January 2012. The Court of Appeals reversed the order given by the Court of First Instance, reasoning that blocking is not effective when the total behaviour of Ziggo customers is taken into account (§5.12). The court introduced a new concept of effectiveness that includes use of other entry points to access illegally offered copyrighted materials, such as the availability of proxy services to go to TPB and also the use of different providers of copyrighted materials (§5.13). From the viewpoint of the administrators of TPB, they are less effective in their infringements due to the blockade (§5.12), but from a more general viewpoint the blockade is not effective. The court is not convinced about the argument that TPB is a test case, since it would have been quite easy for the complaining party (Brein) to add other big torrent providing sites to the affadit (kickass.to, torrentz.eu, Isohunt), as these parties do not have to be involved in the proceedings (TPB was not involved in this case either).

Dutch rights holders' representatives have announced to go to the High Court in a bid for cassation of the judgement to repeal the blocking order. Up until now, they seem wary to start civil procedures against large scale infringing individuals, or stop their efforts to bring large-scale file sharing to a halt.

4. DISCUSSION AND CONCLUSIONS

Where is all this fighting taking us? The EU has issued three directives that aim to provide effective protection of copyright, but the *de facto* situation is that many providers of platforms where copyrighted material can be illegally exchanged are situated outside of EU borders. This means these providers cannot be legally challenged in the EU, as the EU has no jurisdiction. In order to get an effective remedy, the rights holders turned to intermediary service providers, the Internet Access Providers whose customers access the material through the platform located outside the EU.

The Internet Access Providers mostly refuse to cooperate, leading to many court cases in which the rights holders seek orders to block specific websites. In many cases, the court actually grants a blocking order. However, there is a great deal of variety in the way providers have to comply with the order. In Austria, it is thought that the provider is best suited to consider and implement a specific measure. The order is only generically formulated, a practice that introduces legal uncertainty according to these providers (and the Advocate General at the CJEU). In the United Kingdom, providers have been

ordered in great detail how to implement the blocking order. Other EU countries have seen blocking orders with a level of detail in between these two extremes.

Occasionally, no blocking order was granted. In the latest case in The Netherlands, the Appeal Court reversed a previously ordered blockade. The representative of the rights holders (Foundation Brein), has announced it will appeal that decision. Meanwhile the discussion whether blocking websites by Internet Access Providers is effective or not continues. Both sides in the dispute have come up with research showing that their position is correct, while these positions are mutually exclusive: either a blockade is effective or it is not. One further step into the analysis of positions was done by the Dutch Court of Appeal, in that it separated the effectiveness from the viewpoint of the website and the viewpoint of the end user. Whether that provides the answer to the apparent contradiction remains to be seen.

At the moment, EU Member States have a margin of appreciation when implementing the EU Directives 2000/31/EC, 2001/29/EC and 2004/48/EC. The margin leads to differences in case law observed throughout the EU. In light of the ambition that the telecommunications market should be a single market throughout Europe, this seems an anomaly.

Until now, the rights holders' representatives in some EU Member States have shied away from going after the individual. With the rights holders having few other options left, they may in the future choose to start civil procedures against large-scale uploaders. In Germany, a legal practice has emerged in which certain legal firms target thousands of individuals each year. People downloading movies or watching streaming video received letters claiming copyright infringement and a transaction proposal involving hundreds of euros and the signing of a contract to not do it again, ever. Breach of that contract may cost thousands of euros. German government recently adopted a law to maximise the penalty sought, to mitigate the problem (Dedden, 2013).

The judgements of the CJEU are problematic from a copyright enforcement perspective as DPI is the only method currently available to distinguish legal P2P traffic from copyright infringing P2P traffic. Legal use of P2P traffic examples include synchronisation of servers (as Facebook does on its back-office network) and the sharing of Open Source software (such as operating system Linux distributions). Also, the various exceptions in the copyright laws provide for legal transmission of (parts of) copyrighted materials.

The current methods that are imposed by the courts are IP address blocking and DNS blocking. Both are rather crude instruments, indiscriminately blocking legal content and copyright infringing content based on the source. DNS-blocking of websites does not function as a very high threshold since there are sufficient methods available to bypass the blockade (Dilmpieri, King & Dennis, 2011) (Wesselingh, Cristina & Tweeboom, 2013) (Poort, Leenheer, van der Ham & Dumitruc, 2013). IP address blocking appears to do the job, but may only be imposed in cases where an infringing website is the only website behind an IP address. No case law on this subject matter is available today, although the

Yildirim case that was argued before the European Court of Human Rights provides some insight into what direction such case law might go (Yildirim v Turkey, 2012).

Case law is rapidly emerging at the highest level, with several cases before the Court of Justice. So far, the court has interpreted EU Law as prohibiting invasive techniques like Deep Packet Inspection for copyright enforcement. Recently the Court decided that EU Law does not prohibit any blanket type of injunction on third party service providers, with the provisions that lawful information must remain accessible and the measures taken must reasonably effective. These developments will probably lead to the techniques of DNS blocking and IP address blocking being the only tools that may be applied in the future, tools of which the effectiveness is under discussion.

5. BIBLIOGRAPHY

Directives

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (OJ 2000 L 178, p. 1)

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ 2001 L 167, p. 10)

Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ 2004 L 157, p. 45, and corrigenda OJ 2004 L 195, p. 16, and OJ 2007 L 204, p. 27)

European Union, Charter of Fundamental Rights of the European Union, 7 December 2000, OJ L C 364/01, available at: http://www.refworld.org/docid/3ae6b3b70.html [accessed 7 March 2014]

Case law

- A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001), affirming, 114 F.Supp.2d 896 (N.D. Cal. 2000)
- Stockholm District Court, 17-04-2009, Sony Music Entertainment et al v Neij et al, verdict B 13301-06, unofficial translation by IFPI, www.ifpi.org/content/library/pirate-bay-verdict-english-translation.pdf [accessed 28 February 2014]
- Rechtbank Amsterdam (Summary proceedings), 30-07-2009, Brein v The Pirate Bay, case 428212-KG ZA 09-1092, http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2009:BJ4298 [accessed 28 February 2014]

- Hof van Beroep (Court of Appeal) of Antwerp, 26 September 2011, Case 2010/AR/2541 VZW Belgian Anti-Piracy Federation v NV Telenet, m.nt. Van Eecke & Fierens, Larcier RABG 2011/18 pp. 1269-1287
- European Court of Justice, Productores de Música de España (Promusicae) v Telefónica de España SAU 29 January 2008 (Case C-275/06)
- High Court of Ireland, 8 July 2005, [2005] IEHC 233, EMI Records Ireland Ltd v. Eircom PLC, http://www.bailii.org/ie/cases/IEHC/2005/H233.html [accessed 18 December 2013]
- TDC Totalløsninger A/S v. IFPI Danmark asagent for Arcade Music Company et al., UfR 2006.1474 H (Supreme Court of Denmark, 10 February 2006 – Docket no. 49/2005)
- IFPI Denmark as agent for Aller International A/S et al. v. Tele2 A/S (Bailiff's Court of Copenhagen, 25 October 2006-Docket no. F1-15124/2006)
- IFPI Denmark v. DMT2 A/S-Fredriksberg Fogedrets Kendelse, 5 February 2008-FS 14324/2007, unofficial translation by Henrik Spang-Hanssen, Danish Supreme Court attorney-at-law, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1093246 [accessed 27 November 2013]
- Sonofon A/S (tidligere DMT2 A/S) v. IFPI Danmark-Østre Landrets 11. Afdelings kendelse af 26 november 2008 – Kæresag B-530-08, unofficial translation by Henrik Spang-Hanssen, Danish Supreme Court attorney-at-law, http://ssrn.com/abstract=1649682 [accessed 27 November 2013]
- Telenor (tidligere DMT2 A/S og Sonofon A/S) mod IFPI Danmark, Højesterets Kendelse (Supreme Court), afsagt torsdag den 27. maj 2010, Sag 153/2009, UfR 2010:2221-2230
- Hughes, J., and Mady, F. and Bourrouilhou, J., Translation Series: Sabam v. S.A. Tiscali (Scarlet), District Court of Brussels, 29 June 2007, Working paper http://ssrn.com/abstract=1027954 [accessed 24 October 2013], Tiscali later became Scarlet
- Court of Justice of the European Union (CJEU), Reference for a preliminary ruling from the Cour d'appel de Bruxelles (Belgium) lodged on 5 February 2010-Scarlet Extended SA v Société Belge des auteurs, compositeurs et éditeurs (SABAM), Case C-70/10
- Court of Justice of the European Union (CJEU), 24 November 2011, C-70/10, Scarlet Extended NV v Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) (Scarlet-Sabam)
- Court of Justice of the European Union (CJEU), 16 February 2012, C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV (Sabam-Netlog)

- Court of Justice of the European Union (CJEU), 12 July 2011, C 324/09, L'Oréal SA et al v eBay International AG et al (L'Oréal-eBay)
- England and Wales High Court (Chancery Division), 28 July 2011, [2011] EWHC 1981 (Ch), Case No: HC10C04385, Twentieth Century Fox Film Corporation et al v British Telecommunications Plc, http://www.bailii.org/ew/cases/EWHC/Ch/2011/1981.html [accessed 3 March 2014]
- England and Wales High Court (Chancery Division), 27 April 2012, [2012] EWHC 268 (Ch), Case No: HC11C04518, Dramatico Entertainment Ltd et al v British Sky Broadcasting Ltd et al, http://www.bailii.org/ew/cases/EWHC/Ch/2012/268.html [accessed 3 March 2014]
- England and Wales High Court (Chancery Division), 28 February 2013, [2013] EWHC 379 (Ch), Case Nos: HC12F4957, HC12F4958, HC12F4959, EMI Records Ltd et al v British Sky Broadcasting Ltd et al, available @ http://www.bailii.org/ew/cases/EWHC/Ch/2013/379.html [accessed 3 March 2014]
- Court of Justice of the European Union (CJEU), Reference for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 29 June 2012-UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Munich (Germany), Wega Filmproduktionsgesellschaft mbH (Case C-314/12)
- Hearing 20 June 2013, Conclusion of Advocate-General P. Cruz Villalón 26 November 2013, Judgement of the Fourth Chamber 27 March 2014 (Telekabel Wien), http://curia.europa.eu/juris/liste.jsf?language=nl&num=C-314/12 [last accessed 8 May 2014]
- Borgating Court of Appeals (Borgating Lagmannsretts), Nordic Records Norway et al v Telenor ASA (unofficial translation), 9 Feb 2010,
- http://hssph.net/NordicRecords_Telenor_NorwegianCourtofAppeals9Feb2010.pdf [accessed 20 December 2013]
- Court of First Instance The Hague (summary proceedings), 19 July 2010, Stichting Brein v Ziggo and Xs4all, http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBSGR:2010:BN1445 [accessed 3 March 2014]
- Court of First Instance The Hague (Rechtbank 's-Gravenhage), 11 January 2012, case no: 374634/HA ZA 10-3184, Stichting Bescherming Rechten Entertainment Industrie Nederland (BREIN) v ZIGGO B.V. and XS4ALL Internet B.V.,
- http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBSGR:2012:BV0549 [accessed 3 March 2014]
- Court of First Instance The Hague (summary proceedings), 10 May 2012, case no: 413085/KG ZA 12-156, Stichting Bescherming Rechten Entertainment Industrie Nederland (BREIN) v UPC Nederland B.V., KPN B.V., T-MOBILE Netherlands B.V., TELE2 Nederland B.V. and TELE2 Internetdiensten B.V., http://uitspraken.

rechtspraak.nl/inziendocument?id=ECLI:NL:RBSGR:2012:BW5387 [accessed 3 March 2014]

- European Court of Human Rights (ECtHR) second chamber, 18 December 2012, Ahmet Yildirim v. Turkey, request no. 3111/10

Articles and other sources

Website of The Pirate Bay: https://thepiratebay.se/about [accessed 21 February 2014]

Pouwelse J., Garbacki P., Epema D., and Sips H. (2005), *The Bittorrent P2P File-Sharing System: Measurements and Analysis*, in: Castro M. and van Renesse R. (Eds.): IPTPS 2005, Lecture Notes in Computer Science Volume 3640, 2005, pp 205-216

Wolchok S. and Halderman, J. A. (2010), *Crawling BitTorrent DHTs for Fun and Profit*, Proc. of WOOT (Washington, DC, USA, 2010)

Ricketson, S. and Ginsburg, J.C. (2006), *Inducers and Authorisers: A Comparison of the US Supreme Court's Grokster Decision and the Australian Federal Court's KaZaa Ruling*, Columbia Public Law & Legal Theory Working Papers, Paper 0698. Retrieved February 27th, from http://lsr.nellco.org/columbia_pllt/0698

Website of blocked websites UK: https://immunicity.org/blockedsites [accessed 27 February 2014]

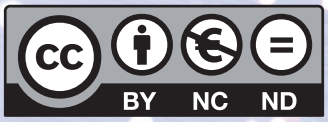
Wesselingh E.M. (2013), Notes from the oral hearing before the Court of Justice of the European Union (CJEU) on 20 June 2013

Dedden M. (2013), *Gesetz gegen unseriöse Geschäftspraktiken – was ändert sich im Urheberrecht?,* 27 June 2013, http://www.mucportal.de/2013/07/01/gesetz-gegen-unseriose-geschaftspraktiken-was-andert-sich-im-urheberrecht/ [accessed 3 March 2014]

Dilmperi A., King T., Dennis C. (2011), *Pirates of the web: The curse of illegal downloading. Journal of Retailing and Consumer Services*, 18 (2) 132-140

Wesselingh, E.M., Cristina, A.S., Tweeboom, N.M.G. (2013), *To Block or Not to Block?*, Working Paper, 4 June 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2273453 [accessed 2 September 2013]

Poort J., Leenheer J., van der Ham J., Dumitruc C. (2013), *Baywatch: two Approaches to Measure the Effects of Blocking Access to The Pirate Bay*, Working paper, 22 August 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2314297 [accessed 2 September 2013]



Internet, Derecho y Política
Una década de transformaciones

Actas del *X Congreso Internacional Internet, Derecho y Política (IDP 2014)*

ISBN: 978-84-697-0826-2

Para citar la obra, por favor, utilicen las siguientes referencias indistintamente:

Balcells Padullés, J., Cerrillo-i-Martínez, A., Peguera, M., Peña-López, I., Pifarré de Moner, M.J. & Vilasau Solana, M. (coords.) (2014). *Internet, Derecho y Política. Una década de transformaciones*. Actas del X Congreso Internacional Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona, 3-4 de julio, 2014. Barcelona: UOC-Huygens Editorial.

Balcells Padullés, J., Cerrillo-i-Martínez, A., Peguera, M., Peña-López, I., Pifarré de Moner, M.J. & Vilasau Solana, M. (coords.) (2014). *Internet, Law & Politics. A Decade of Transformations*. Proceedings of the 10th International Conference on Internet, Law & Politics. Universitat Oberta de Catalunya, Barcelona, 3-4 July, 2014. Barcelona: UOC-Huygens Editorial.

http://edcp.uoc.edu/symposia/lang/es/idp2014/proceedings/

UOC
Universitat Oberta de Catalunya
www.uoc.edu

HUYGENS
EDITORIAL