Univerzita Karlova v Praze
Právnická fakulta

Storm in the Safe Harbor

From Passive-Reactive to Active-Preventive ISPs and Back

Studentská vědecká a odborná činnost

Kategorie: magisterské studium

2014
VII. ročník SVOČ

Autor: Vojtěch Mlynář
Konzultant: JUDr. Petra Žikovská

Storm in the Safe Harbor

From *Passive-Reactive* to *Active-Preventive* ISPs and Back

Vojtech Mlynar

Introduction

There has been a storm in the safe harbors for Internet Service Providers (ISPs). Since formation of the Internet, ISPs have been under pressure to assume more liability for information they transmit or store. The content owners tried to push ISPs in the same position as off-line content publishers with strict liability regime for defamatory content or copyright infringement in an online environment. Although policy makers and judicial decisions pushed back against ISPs liability for online content, the pressure continues.

Today, the focus is shifting from the Internet's content to the Internet's infrastructure. As its name suggests, the Internet consists of endless number of interconnected networks. Stoping infringement at one place usually means the perpetrator will change its location and continue from a different location on the network. It may be easier for the European courts to order regional Internet access providers to simply block access to these 'dark places' of the Internet. The recent decision of the European highest court confirmed the trend, once again rising waves in waters of the ISPs' safe harbors.

In this paper, I will discuss developments pertaining to ISPs' liability for copyright infringement in the European Union (EU). In Section (I), I will briefly explain basic roles of ISPs and the EU law providing safe harbors for ISPs. In Section (II), I will outline how these rules were interpreted in judicial decisions in the EU Member States and what position was subsequently taken by the Court of Justice of the European Union (CJEU). I will examine the recent judgement of the CJEU concerning the new EU rules for website-blocking injunctions. Finally, I will point out some disturbing elements of the latest judgement and conclude the paper with suggestions of broader implications of the judgement.

I. ISP's Role on the Internet

A. ISP Primer

ISPs are the basic players of the Internet. They cover wide range of activities which take place in an online world. In fact ISPs *are* the Internet. Without them the Internet would not work.

To make things simple, we can divide ISPs into two basic categories. First, ***access* ISPs** who provide basic infrastructure for the Internet. These are roads, highways, power lines and pipe lines of the cyberspace. Their main job is to provide access to communications networks and facilitate transmission of information between various points within these networks.[1] The second category can be characterized as online content providers - ***content* ISPs**. This group offers diverse Internet services, but the underlaying service is online storage of data - hosting.[2]

B. The Legal Framework

To protect ISPs position and growth of the Internet, at the beginning of the new century, the European Union adopted legislation protecting ISPs' from liability for copyright infringement occurring on their networks. The Directive 2000/31/EC (eCommerce Directive)[3] introduced safe harbor provisions to protect online intermediaries from traditional liability for information passing through and residing on their networks.[4]

The eCommerce Directive prohibits general content monitoring obligations to be placed on ISPs.[5] It does not require ISPs to actively manage passing traffic or police content residing on their networks. Instead, the liability regime is based on *passive-reactive* approach. An ISP

[1] They can be further divided into Tier-groups, based on potential reach of their networks and amount of traffic they handle. Tier-1: large "backbone" network operators; and Tier-2/3: local distributors or interconnectors. Interestingly, while in an 'off-line' world EU law requires backbone infrastructure operators (Tier-1) to act as separate entities in order to ensure fair competition and non-discriminatory access to main networks, no such requirements exist in an online environment. *See e.g.:* EU rules requiring main gas transmission operators to be incorporated as separate entities: Article 9 of the Directive 2009/73/EC *on common rules for the internal market in natural gas*, OJ L 211.

[2] These data will take various forms for an Internet end-user, *e.g.*, an email account, a traditional website (www.whitehouse.gov), a photo or video sharing service (Flickr, Youtube), social media (Twitter, Facebook), cloud computing applications (Google-drive, iCloud), file-sharing servers (Rapidshare, Megaupload), *etc.*

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

[4] Prior to the eCommerce Directive, statute featuring nearly-identical provisions was adopted in the U.S.: *Digital Millennium Copyright Act* (DMCA), 17 U.S.C.A. § 512. Today, similar rules are in place worldwide, *see*: Jeremy de Beer, Christopher D. Clemmer, *Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries*, 49 Jurimetrics 375 (2008-2009).

[5] Article 15 of the eCommerce Directive.

intervenes only when it gains actual knowledge about an infringing activity, typically upon notice of alleged copyright violation by a third party. Otherwise, an ISP remains neutral and passive.[6]

The DMCA and the eCommerce Directive divide ISPs' activity into three types of conduct: (i) mere conduit, (ii) caching and (iii) hosting. These activities are related to each other and one intermediary can engage in all off these activities at the same time.

(1) Mere conduit[7]

First type of conduct deals with situations where ISPs act as mere conduits, *i.e.* carriers of transitory digital network communication. ISPs are protected against any liability potentially arising from transmitted content, provided that they are only *passively* involved in the transmission. Any interference with transmitted information, *e.g.*, monitoring content, selecting recipients or initiating the transmission, may result in loss of the liability protection. Typically, access ISPs act as *mere conduits*, transporting data from one point on the network to the other.

(2) Caching[8]

Caching is defined as automatic, intermediate and temporary storage of data on an ISP's servers, performed for the sole purpose of effective transmission of information from one point on the network to the other. While transmitting information from point "A" to point "B", it may be necessary for an ISP to create several copies along the way. Other times, an ISP may create a temporary copy to facilitate faster access to information stored on distant servers. Due to ISPs' caching, users benefit from faster access to information they seek and ISPs can significantly reduce network workload and congestion.

Again, the eCommerce Directive includes specific provisions which ISPs have to abide. As long as intermediaries act *passively* and neutrally (*i.e.*, automatically cache data without monitoring its content), they will not be liable for copyright infringing material in their caches.

[6] The wording of the eCommerce Directive does not prevent ISPs from active content monitoring. However if ISPs do monitor, they will not be shielded from liability for third-party content, as it could be argued an ISP gained *actual knowledge* about illicit content through its monitoring activity.
[7] Article 12 of the eCommerce Directive.
[8] Article 13 to the eCommerce Directive.

If they become aware of infringing content, they have to react and expeditiously remove illicit content from their systems.

(3) ***Hosting***[9]

While transitory communication and caching deal with temporary storage of information, hosting providers store third-party content for potentially indefinite period of time. The liability-exemption regime is similar to caching and again requires *passive-neutral* approach. Additionally, to be shielded from liability, hosting providers cannot be aware of facts or circumstances from which infringing activity is apparent. This requirement, also referred to as 'red-flag' knowledge,**[10]** turns on whether the ISP was subjectively aware of facts that would have made the infringement objectively obvious to a reasonable person.**[11]**

Interestingly, contrary to *mere conduit* and caching, hosting liability protection does not require intermediaries to remain fully *passive*. To certain extent, ISPs offering hosting services can modify information uploaded on their servers without piercing their liability shield.**[12]**

(4) Notice-and-takedown

As already noted above, online intermediaries cannot be required to perform general monitoring of content residing on or passing through their systems. Instead, in most cases hosting providers become aware of infringing activities through *notice-and-takedown*. This procedure ensures copyright owners are able to bring infringing material to an ISP's attention. When hosting provider becomes aware of unlawful material hosted on its systems, it has to act *expeditiously* to remove or block access to infringing material. While the U.S. DMCA statute offers detailed rules specifying elements of these notifications,[13] the eCommerce Directive has no such guidance and leaves notice requirements and its interpretation to individual member states. As a result, *notice-and-takedown* procedures are fragmented across the EU Member States (sometimes even within the same Member State).[14] As a result, intermediaries are forced

[9] Article 14 of the eCommerce Directive.
[10] Edward Lee, *Decoding the DMCA Safe Harbors*, 32 Colum. J.L. & Arts 233 (2008-2009).
[11] *See* reasoning in: *Capitol Records, LLC, EMI Blackwood Music, INC., et al. v. Vimeo, LLC*, Dist. Court, SD New York (31 December 2013).
[12] There is no clear delineation between *neutral* interaction and data management which may lead to *actual knowledge* about data's content. The extent to which an ISP may manage data hosted on its servers is subject to ongoing debate. *See e.g.*: Patrick Van Eecke, *Online service providers and liability: A plea for a balanced approach* (2011) 48 Common Market Law Review, Issue 5, p. 1481;
[13] 17 U.S.C.A. § 512 (c)(3).
[14] Notwithstanding the fact there is no uniform notice-and-takedown procedure, EU rules and case law provide at least minimum requirements for ISPs. Article 5(1)(c) of the eCommerce Directive requires service providers to supply recipients

to tailor their services differently for each Member State and users' experience may vary.[15] This situation not only directly conflicts with aims stated in the eCommerce Directive,[16] but, more importantly, creates significant legal uncertainty for Internet intermediaries who wish to provide uniform services across the EU.

II. From *Passive-Reactive* to *Active-Preventive* and Back

While statutory language of the eCommerce Directive requires ISPs to remain in neutral position with *passive-reactive* approach to copyright infringement, judicial interpretation of these rules can produce very different outcomes. In this section, I will examine the most important decisions and policy initiatives influencing ISPs neutral position and the push for *active-preventive* ISPs. In will further examine response of the Court of Justice of the European Union (CJ) with the focus on its recent decision in *UPC Telekabel Wien* and its implications for Internet access providers.

A. Judicial Decisions in EU Member States

All EU Member States transposed rules introduced in the eCommerce Directive into their national legislation.[17] While purpose of the eCommerce Directive was to ensure uniform treatment of Internet intermediaries throughout the EU, the reality proved to be different. It did not take long and the EU's "area without internal frontiers for information society services"[18] was slipping into country-specific legal regimes with significant differences.

---

of their service with contact information. According to decision of the Cour of Justice of the European Union, in addition to e-mail address service providers must provide *"other information which allow them to be contacted rapidly and communicated with in a direct and effective manner";* Case C-298/07, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v deutsche internet versicherung AG*, OJ C 313.
In January 2012 the EU Commission launched public consultation on *notice-and-takedown* procedures, the purpose of consultation was to gather opinions of different parties and establish best practices, results of these conclusions were not yet published, see: http://ec.europa.eu/internal_market/e-commerce/notice-and-action/index_en.htm (last visited Mar 26, 2014).

[15] Verbiest, Spindler, Riccio and Van der Perre, *Study on liability of Internet intermediaries*, study prepared for the European Commission - Markt/2006/09/E Service Contract ETD/2006/IM/E2/69 (12 November 2007).

[16] Recital 1 of eCommerce Directive reads: "*[T]he development of information society services within the area without internal frontiers is vital to eliminating the barriers which divide the European peoples.*"

[17] *Study on liability of Internet intermediaries*, op. cit. *supra* note 15.

[18] Recital 1 of the eCommerce Directive.

(1) French Leading the Way - In the Wrong Direction

In *Lafesse v. MySpace*[19] the Civil Court of Paris held MySpace liable for copyright infringement despite the apparent fact that MySpace acted as a typical hosting provider. The court found that MySpace allowed its users to create personalized webpages, offered special tools for uploading content (including video) and generated profits from advertisements placed alongside videos uploaded by users. These factors were enough for the court to consider MySpace as a *publisher*, liable for infringing content uploaded by its users. The court decided MySpace stepped outside safe harbor provisions of Article 14 of the eCommerce Directive[20] and was therefore not eligible for liability protection.

One month later, the same Civil Court of Paris considered DailyMotion[21] (a video-sharing website) not to be a *publisher*, despite evident similarities of its services with the ones of MySpace - including commercial advertising alongside uploaded videos. Although the court qualified DailyMotion as an ISP and not a *publisher*, nevertheless, the ruling was even more catastrophic for online intermediaries then the previous decision in *Lafesse*. The court ruled DailyMotion was not protected from liability, because it *must have known* the illegal content was present on its website. Since the service provider *should have been* aware its service was being used for copyright infringement, it had a duty to implement technical measures to prevent all unlawful activities on its website.[22] Consequently, according to the Court of Paris and contrary to the eCommerce Directive, ISPs must *actively* prevent copyright infringement.

(2) Take-Down/Stay-Down - Going Further in the Wrong Direction

In Z*adig v. Google*,[23] another well known French case, brought by French documentary producer against Google Video, the Court of Paris found Google liable for copyright infringement, despite the fact Google complied with *notice-and-takedown* procedures. The plaintiff argued, once a hosting provider is notified of specific instance of infringement, it has a duty to prevent future re-postings of the same infringing content. Google contested it was exempted from liability under Article 14 of the eCommerce Directive, because it had no knowledge of the specific infringement and, upon receiving formal notice, acted expeditiously

[19] *Lafesse v. Myspace*, Tribunal de Grande Instance Paris [Civil Court of Paris], ref. 22 June 2007 (Fr.).
[20] Implemented in the French law as Article 6.I.2 of the *French Act on Confidence in the Digital Economy* (21 June 2004).
[21] *Nord-Ouest Production v. S.A. DailyMotion and S.A. UGC Images*, Tribunal de Grande Instance Paris [Civil Court of Paris], ref. 13 July 2007 (Fr.).
[22] Nicolas Jondet, *The silver lining in Dailymotion's copyright cloud*, University of Edinburgh, juriscom.net (19 April 2008), available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1134807.
[23] *Zadig Productions v. Google Inc.*, Tribunal de Grande Instance Paris [Civil Court of Paris], ref. 19 October 2007 (Fr.).

to remove the illicit content. The court sided with the plaintiff and imposed a duty on Google to implement all technical means necessary to avoid further dissemination of illicit content.

To avert direct conflict with prohibition of general monitoring obligation in Article 15 of the eCommerce Directive, the court considered these measures to be a "targeted and temporary surveillance" aimed at avoiding damage caused by *specific* content.[24] In practice, the decision in *Zadig* meant ISPs had to adopt technological controls that *actively* prevent, rather then *passively* react to, alleged illegitimate content. This duty, referred to as "*take-down/stay-down*",[25] was subsequently confirmed in decisions of the French Court of Appeals in number of cases including Google as a defendant.[26]

(3) Changing the Course

In 2012, the *take-down/stay-down* rule was rejected by the Court de Cassation, France's highest civil court, in *Google v. Bac Films*[27] involving (again) Google Video service. The court ruled that the duty to prevent reposting of infringing content is equivalent to general obligation to monitor and therefore prohibited by Article 15 of the eCommerce Directive.

However, the decision in *Google v. Bac Films* introduced another disturbing element for online intermediaries. The court's reasoning suggested Google could be held liable for unlawful reproduction and public performance of copyrighted works.[28] The court recognized the infringing content was stored on third-party servers, but because Google made the content accessible directly through its own website (by framing and deep-linking), it went beyond "simple technical functions" and was therefore not protected from liability under the eCommerce Directive. Same reasoning was adopted in the another decision of the same court regarding "Google Suggestions" search term function.[29] The court's requirement that ISPs

[24] de Beer, Clemmer, op. cit. *supra* note 4.
[25] *See e.g.:* Jane C. Ginsburg, *Take Down/Stay Down: RIP in France? But Little Solace for Google…*, Aug 6, 2012, The Media Institute, available at: http://www.mediainstitute.org/IPI/2012/080612.php; Zohar Efroni, *Take Down Stay Down*, The Center for Internet and Society, Stanford Law School (14 May 2007), available at: http://cyberlaw.stanford.edu/blog/2007/05/take-down-stay-down.
[26] *Google Inc. v. Compagnie des phares et balises; Google Inc.v. Bac Films, the Factory; Google Inc.v. Bac Films, the Factory, Canal+; Google Inc. v. Les Films de la Croisade, Goatworks Films*; all issued by Cour d'appel de Paris [Paris court of appeals], ref. 14/1/2011, available at: http://www.legalis.net (last visited Mar 30, 2014).
[27] *Google France v. Bac Films*, Cour de cassation Première chambre civile [Highest civil law court], decision No. 831 ref. 12/7/2012 (Fr.), available at: http://www.courdecassation.fr/jurisprudence_2/premiere_chambre_civile_568/831_12_23883.html (last visited Mar 31, 2014).
[28] The French court did not address the issue directly because the plaintiff did not assert these claims.
[29] *Syndicat national de l'édition phonographique v. Google*, Cour de cassation Première chambre civile [Highest civil law court], decision No. 832 ref. 12/7/2012 (Fr.); Jane C. Ginsburg, op. cit. *supra* note 25 (discussing decision in *Google France v. Bac Films*).

perform only "simple technical functions" in order to qualify for liability exemption does not reflect wording of the eCommerce Directive and can hardly be reconciled with services intermediaries offer in Web 2.0 environment.

The issue was recently addressed by the CJ in its judgement in *Svensson v Retriever Sverige AB.*[30] The CJ held hyperlinking freely available copyrighted content cannot be considered as an unlawful 'communication to the public', as defined by the InfoSoc Directive.[31] Therefore, ISPs are not liable for copyright infringement through links to content residing on third-party websites, unless they become aware that the link leads to illicit content, or unless the link would make it possible "to circumvent restrictions put in place by the site on which the protected work appears in order to restrict public access to that work [only] to the (…) sites subscribers."[32]

B. The Court of Justice Strikes Back

So far, the Court of Justice of the European Union had a chance to rule on interpretation of ISPs liability and protection offered by the eCommerce Directive only in several cases. *Promusicae*[33] was the first case where CJ dealt specifically with tension between data protection and online enforcement.

(1) The Proportionality Test

Promusicae, the spanish organization of producers and publishers of musical and audiovisual recordings, demanded Telefónica (access ISP) to hand over records identifying users who were allegedly infringing Promusicae's copyright through file sharing software. Promusicae sought to obtain user-identifying records to launch a civil lawsuit against individual users. Telefónica held these records pursuant to the EU Data Retention Directive,[34] which requires access ISPs to store user-identifying data (date, time and IP addresses of users'

[30] Case C 466/12, *Svensson v Retriever Sverige AB*, (13 February 2014, not yet published in the Official Journal).
[31] Directive 2001/29/EC *on the harmonisation of certain aspects of copyright and related rights in the information society*, O.J. L 167/10.
[32] Case C 466/12, para. 31, op. cit. *supra* note 30.
[33] Case C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, OJ C 64
[34] Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, OJ L 105 (the Data Retention Directive).

internet traffic) that can be used by law enforcement authorities to combat serious crimes.[35] The CJ set up a proportionality test. The court emphasized, national rules must be proportionate and strike a fair balance between fundamental rights protected by EU law (in this case, right to property and privacy). The proportionality requirement set up in *Promusicae* has been subsequently used in following cases before the CJ.

(2) Active Monitoring Obligation

While French courts have been very active in their decisions concerning online intermediaries, the most controversial decision was handed down by the Belgian court in case *SABAM v. Scarlet*.[36] The Belgian court ordered access ISP Scarlet to implement technical measures which would make it impossible for its subscribers to send or receive music files (held by SABAM - the Belgian Society of Authors, Composers and Publishers) through P2P file sharing software. Unlike French cases which targeted content ISPs, *SABAM v. Scarlet* was the first European case where court imposed active monitoring obligation on an access ISP. Because the ruling of the Belgian court apparently contradicted prohibition on general monitoring contained in Article 15 of the eCommerce Directive,[37] the matter was referred to the CJ for a preliminary ruling.[38]

The CJ held an ISP cannot be ordered to install filtering and blocking systems to prevent transfer of potentially infringing files. The court reasoned such requirement would oblige ISPs "to actively monitor all the data relating to each of its customers in order to prevent any future infringement of intellectual-property rights. It (…) would require the ISP to carry out general monitoring, something which is prohibited by [the eCommerce Directive]."[39] The CJ recalled

[35] In the recent decision, the CJ declared the Data Retention Directive invalid due to its "wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data." *See* joined Cases C 293/12 and C 594/12, *Digital Rights Ireland*, (8 April 2014) [not yet published in the Official Journal].
[36] *SABAM v. Scarlet* (formerly Tiscali), Tribunal de premiere instance de Bruxelles [Court of First Instance Brussels], 18 May 2007 (Belg.), for English 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. (2008), available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1027954.
[37] In the questionable reasoning, the Belgian judges issuing the injunction seem to argue they do not have to consider prohibition on general monitoring since it only applies in decisions concerning ISP's liability, whereas injunction reliefs do not examine liability issues. Moreover, the judges argued "blocking and filtering certain information" does not amount to monitoring. See the translation, *Id.*, pp. 8-9; *see* also: Patrick van Eecke, op. cit. *supra* note 12, pp. 1459-1461.
[38] Case C-70/10, *SABAM v. Scarlet Extended SA*, (24 November 2011).
[39] *Id.*, para. 40.

the proportionality test from its decision in *Promusicae* and also relied on the Charter of Fundamental Rights of the European Union:[40]

> *"Moreover, the effects of that injunction would not be limited to the ISP concerned, as the contested filtering system may also infringe the fundamental rights of that ISP's customers, namely their right to protection of their personal data and their freedom to receive or impart information, which are rights safeguarded by Articles 8 and 11 of the Charter respectively."*[41]

SABAM v. Scarlet was followed by the second ruling involving SABAM where the plaintiff sought broad "filtering" injunction against Belgian social media platform Netlog.[42] Although the facts were similar to previous ruling, the decision was highly anticipated because it was not clear whether the CJ will extend the *SABAM v. Scarlet* reasoning (concerning an access ISP) to services offered by content ISPs. Indeed, the court applied same reasoning as in *SABAM v. Scarlet*. The CJ held the injunction was not proportionate and violated the 'no obligation to monitor' principle of the eCommerce Directive as well as the ISP's freedom to conduct business, users' personal data protection and freedom of information set out in the EU Fundamental Rights Charter.[43]

Both *SABAM* rulings are significant as they effectively draw a boundary for national courts of the EU Member States in imposing injunctions against online intermediaries. The CJ rejected the shift towards *active-preventive* ISPs and set a course for uniform interpretation of the eCommerce Directive. However, practical impacts of the CJ's rulings remain to be seen. In fact, the first 'rebelling' judgement was already handed down by the German Bundesgerichtshof (the German Supreme Court) in *GEMA v. RapidShare AG.*[44]

In August 2013, more than one year after the CJ's second decision in *SABAM*, the German court held that RapidShare - provider of an online file-hosting service - has a duty to *actively* monitor its service for infringement. RapidShare was required to employ additional monitoring measures and conduct a "market monitoring" to actively search for links to infringing files using publicly available resources, such as search engines, discussion forums and social media.

---

[40] *Charter of Fundamental Rights of the European Union*, (26 October 2012), O.J. 2012/C 364/01 (the EU Fundamental Rights Charter).
[41] Case C-70/10, para. 43, op. cit. *supra* note 38.
[42] Case C-360/10, *SABAM v. Netlog NV* (16 February 2012).
[43] *Id.*, para. 44-51.
[44] *GEMA v. RapidShare AG*, Bundesgerichtshof, Case No. I ZR 80/12 (Aug. 15, 2013) (Germany).

The German court acknowledged liability protection for ISPs under the eCommerce Directive but relied on Recital 48 which permits Member States to "requir[e] service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities." Although there is little doubt RapidShare services were predominantly used for illegal file sharing, the measures imposed by the German court can hardly be reconciled with the CJ's decisions in *SABAM*. So far, the CJ did not offer any counter response to the German ruling.

(3) Website Blocking

While *SABAM* decisions concerned blocking of access to *specific* content uploaded by, or transferred between users, the recent judgement of the CJ went a step higher. In *UPC Telekabel Wien*[45] the CJ was asked to decide whether access ISPs can be required to block access to infringing websites altogether. The Austrian court issued an injunction requiring an ISP to block access to third-party website infringing plaintiffs' copyright. Because the website was hosted on servers outside the EU, and therefore outside effective reach of Austrian authorities, plaintiffs brought their case against Austrian internet access provider UPC, asking it to prevent its subscribers from accessing the website.

Plaintiffs based their claim on provisions of the EU law, which require Member States to ensure right holders can "apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right."[46] The ISP argued the term "intermediary" should be limited to content ISPs that made infringing materials available online, and should not apply to access ISPs which merely connect end-users to the Internet. Instead, content owners should seek remedies against the actual infringer, *i.e.*, the website operator.[47] The CJ rejected the distinction and ruled it legal under EU law to impose website-blocking obligations on access ISPs. According to the court's reasoning, access ISPs must be considered intermediaries "whose services are used to infringe a copyright" and, therefore, may be subject to website-blocking injunctions.[48]

---

[45] Case C-314/12, *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, Wega Filmproduktions-gesellschaft mbH*, (27 March 2014).
[46] Article 8(3) of the InfoSoc Directive, op. cit. *supra* note 31.
[47] In fact, the website at issue (kino.to) ceased operation in June 2011 - long before the CJ's judgement - following an action of the German police forces against its operators. *See: UPC Telekabel Wien*, para. 13, op. cit. *supra* note 45.
[48] Case C-314/12, para. 32, op. cit. *supra* note 45.

The court went on to asses impact on fundamental rights and freedoms enshrined in the EU Fundamental Rights Charter. The CJ concluded that a website-blocking order does not infringe these rights as long as the choice of appropriate blocking-measures is left with ISPs and internet users are not deprived of access to lawful content.[49]

The decision puts ISPs in a difficult position. Simply as a result of connecting its subscribers to the Internet, every single access ISP in the EU is now effectively considered "an intermediary whose services are used to infringe a copyright."[50] Should a court issue an injunction, an ISP would be in a dilemma. On the one hand, an ISP must adopt measures which are "sufficiently effective to ensure genuine protection" of right holders, *i.e.*, effectively block access to infringing website.[51] On the other hand, an ISP "must ensure compliance with the fundamental right of internet users to freedom of information."[52] If an ISP employs measures that are easy to circumvent it will risk sanctions for non-compliance. If an ISP employs blocking measures that are too wide it will risk liability for violating freedoms of its customers.[53] The CJ did not offer any guidance on this dilemma. It is for national courts to determine whether a proper balance was struck between the two opposing obligations. Arguably, this may result in a situation where ISPs will be held to different standards across the EU Member States.

Surprisingly, the court did not discuss the monitoring prohibition of Article 15 of the eCommerce Directive. A short analysis can be found in the Opinion of Advocate General Villalón who argued the injunction only concerns a specific website and for this reason does not involve monitoring obligation.[54] The CJ considered access ISPs to be best situated to put an end to copyright-infringing off-shore websites where other remedies are not available to right holders or would not be as effective. While this may be true, the CJ's *'end justifies the means'* logic in effect shifts responsibility for copyright policing onto innocent parties, who will be required to employ significant costs and effort implementing these injunctions.

---

[49] *Id.*, para. 54-64.
[50] Copyright owners do not even need to demonstrate that some of the ISP's customers were actually accessing an infringing content online. For a court to issue a blocking-injunction it merely suffice the possibility of accessing an infringing website exists. *See Id.*, para. 36.
[51] *Id.*, para. 62-63.
[52] *Id.*, para. 55.
[53] The CJ stressed the national procedural rules must provide a possibility for the ISP's customers to assert their rights before a court once blocking measures taken by the ISP are known. See *Id.*, para. 57.
[54] Case C 314/12, Opinion of Advocate General Cruz Villalón, Nov 26, 2013, para. 77-78.

Even before the decision in *UPC Telekabel Wien*, courts in UK and in France ordered access ISPs to block off-shore P2P file sharing websites (including well known Pirate Bay).[55] In some instances, the blocked websites functioned as mere aggregators, providing links to video-streams hosted on other websites.[56] In all of these cases, courts argued that in the absence of alternative effective reliefs, it is justified to require access ISPs to block infringing websites. With the CJ decision backing the practice, we can soon expect right holders (especially audio and video industries) to take a full advantage of the newly available blocking tool, even in countries where judges were so far reluctant to issue website-blocking injunctions.[57] The website-blocking will likely become a widely requested remedy for copyright infringement across the EU.

(4) Is Website-Blocking an Effective Remedy?

It is hard to asses how effective the blocking measures can be in practice. For example, blocking domain name and IP address of illicit website can be easily circumvented by website owners as well as end-users.[58] Indeed, evident inefficiency of website-blocking measures was already recognized in the decision of the Dutch Court of Appeals[59] issued prior to the CJ's *UPC Telekabel Wien* case. The Dutch court observed that blocking had only minimal impact on users' behavior and ordered the injunction to be lifted immediately. While the Dutch decision demonstrates courts pay attention to practical (in)effectiveness of issued injunctions, it is easy to imagine a court could rule in the opposite direction: requiring an ISP to take additional measures and make blocking more effective. As already noted above, the CJ did not offer any guidance on the proportionality test in the *UPC Telekabel Wien* decision. Thus, it is solely to national courts to determine which measures are reasonable to expect from ISPs implementing

[55] *See e.g.: Twentieth Century Fox Film Corp & Ors v British Telecommunications Plc* [2011] EWHC 1981 (Ch) (28 July 2011) (UK); *Dramatico Entertainment Ltd v British Sky Broadcasting Ltd* [2012] EWHC 268 (Ch) (20 February 2012) (UK); *The Football Association Premier League Ltd v British Sky Broadcasting Ltd & Ors* [2013] EWHC 2058 (Ch) (16 July 2013) (UK); A*PC et autres v. Auchan Telecom*, Tribunal de Grande Instance Paris [Civil Court of Paris], ref. 28/11/2013 (Fr.).
[56] *The Football Association Premier League Ltd v British Sky Broadcasting Ltd & Ors*, *Id.*, para. 6.
[57] *See, e.g.:* an Irish case where the judge refused to issue an injunction due to lack of statutory support for such measure, although he found the relief to be merited on the facts: *EMI Records (Ireland) Ltd & Ors v. UPC Communications Ireland Ltd* [2010] IEHC 377 (11 October 2010) (Ir.), para. 138.
[58] Websites may easily relocate their content to a different server with the new IP address and domain name. Users have various options to circumvent blocking measures, for a basic overview, see "*Internet censorship circumvention"* article on Wikipedia: http://en.wikipedia.org/wiki/Internet_censorship_circumvention.
[59] *Ziggo BV, XS4All Internet BV v. Stichting Bescherming Rechten Entertainment Industrie Nederland Brein*, Gerechtshof Den Haag ECLI: NL: GHDHA: 2014:88 (28 January 2014) (Nl.).
According to the study of dutch researches relied upon in the courts ruling, only 4 to 6 percent of users have decreased their downloading activity as a result of the blocking. See: Cyrus Farivar, *Blocking doesn't work: Dutch court lifts Pirate Bay ban*, Ars Technica (28 January 2014), available at: http://arstechnica.com/tech-policy/2014/01/blocking-doesnt-work-dutch-court-lifts-pirate-bay-ban/.

the blocking injunction. In jurisdictions which already demonstrated their willingness to take tougher stance agains ISPs liability, *e.g.*, France and UK, stricter and broader blocking requirements are much more likely to occur.

More importantly, blocking entire websites inevitably risks blocking legitimate content too. Imagine a website with equal amount of illicit and legitimate content. Should these sites be regarded as 'dedicated to infringement' and therefore subject to blocking injunctions? What if 90 percent of a website is legitimate content, *e.g.*, photos of cute puppies and kittens, and 10 percent illegitimate, *e.g.*, latest Hollywood movie. Would it be proportionate for a court to order blocking based on these 10 percent? But what if the 10 percent of illicit content attracts 90 percent of the website's traffic?[60] These are all important questions which were left for national courts to adjudicate, generating, once again, substantial legal uncertainty for ISPs across the EU.

III. Conclusion

Preventing copyright infringement on the Internet may seem like a futile exercise. Frustration among content owners often drives litigation against online intermediaries, instead of focusing on individual perpetrators. Some national courts seem to have more empathy for (national) content owners than for (international) ISPs who often benefit, though not always intentionally, from copyright infringing activities on their networks. While stoping copyright infringement is a legitimate goal, national courts often overlook broader implications of their decisions for an online environment, creating a storm in the safe harbors provided by eCommerce Directive for online intermediaries.

The Court of Justice of the European Union cleared out the stormy weather and once again made the safe harbors secure place, where passive and neutral ISPs are shielded from liability for copyright infringement. But even the CJ has empathy for European content owners. Although the consequences of the CJ's latest judgement in *UPC Telekabel Wien* remain to be seen, it certainly caused some waves to appear in waters of safe harbors.

Meanwhile, it is becoming more apparent litigation is not the most effective way to solve problems of copyright owners. Instead, content owners and ISPs are finding a common ground

[60] Jane C. Ginsburg, *Copyright Enforcement in the EU: The Return of Website Blocking*, The Media Institute, Dec 30, 2013, available at: http://www.mediainstitute.org/IPI/2013/123013.php

and collaborate to prevent copyright infringement online. Notwithstanding the fact that motivations on each side may be different, the results of these collaborations are often similar to those sought by copyright owners in litigations.[61] Content owners also increasingly cooperate directly with Internet access providers in various 'educational' campaigns.[62] These initiatives and voluntary collaborations may be beneficial for all parties involved, including Internet end-users. Positive effects of enhanced collaboration are clearly demonstrated on declining levels of illegal file-sharing, as Internet users are utilizing newly available online services.[63] However, it is important to ensure transparency and public oversight in these deals.[64] Today, the debate about role of Internet Service Providers is focused on copyright infringement - an important aspect of ISPs conduct. Nevertheless, it is important to keep in mind other important aspects of online environment and the implications copyright enforcement may have. These include issues of privacy,[65] freedom of information[66] or network neutrality.[67] Creating the policy for online intermediaries centered around the copyright

[61] The prime example of such collaboration, practically implementing measures successfully contested by ISPs in court, is the video 'fingerprinting' technology used by YouTube. These measures in practice prevent re-postings of infringing videos - a remedy sought by plaintiffs, *e.g.*, in *SABAM v. Netlog*, or in *Zadig v. Google*. Another recent example is the cloud storage service Dropbox which deploys similar file-fingerprinting measures to prevent users from sharing copyrighted files.
Motivation of copyright owners is simply to stop illegal file sharing in hope users will then pay for the content available through legal means. ISPs motivations are often unrelated to copyright infringement. Instead ISPs may wish to manage the content on their websites in more efficient way (often making money in the process). For example, YouTube wants to adjust advertising displayed alongside user-uploaded videos to be able to generate more revenue from these targeted advertisements. Whereas Dropbox wants to effectively manage content to enhance its storage capabilities and reduce network congestion. But managing content in this way implies ISPs may be held liable for copyright infringement as they become actually aware of the content (including illicit content) residing on their servers. Therefore, these ISPs are motivated to reach a deal with copyright owners.
See: Youtube's support page, explaining its "Content ID Match", available at: http://youtube.com/yt/copyright/?rd=1; Kyle Orland, *Dropbox clarifies its policy on reviewing shared files for DMCA issues*, Ars Technica (30 March 2014), available at: http://arstechnica.com/tech-policy/2014/03/dropbox-clarifies-its-policy-on-reviewing-shared-files-for-dmca-issues/.
[62] *E.g.:* Cooperation of U.S. major access ISPs and large content-owners associations in: the Center for Copyright Information (http://www.copyrightinformation.org); or cooperation between major access ISPs, content owners, government and telecoms regulator in UK: *Net firms in music pirates deal*, BBC (24 July 2008), available at: http://news.bbc.co.uk/2/hi/technology/7522334.stm.
[63] Consider, for example, various free or subscription based music and video streaming services, such as Spotify, Pandora, iTunes Radio, Netflix or Hulu. These services made 'traditional' illegal music sharing inconvenient and unnecessary even for many stubborn 'pirate' downloaders. *See e.g.:* Hayley Tsukayama, *Music piracy on the decline as digital music sales grow*, The Washington Post (February 26, 2013); Sophie Curtis, *Spotify and Netflix curb music and film piracy*, The Telegraph (18 July 2013).
[64] Although Virgin Media (one of the ISPs involved in the cooperation deal in UK) claimed its campaign is merely educational, first round of 'educational' letters to alleged illegal downloaders featured a large red sticker saying: "*Important - if you don't read this, your broadband could be disconnected.*" Virgin Media later removed the sticker and blamed its placement on envelopes on administrative mistake. The company later expressed it had no intention to disconnect its customers from the Internet. *See:* Claudine Beaumont, *Virgin Media blames 'administrative oversight' for threats on warning letters*, the Telegraph (4 July 2008), available at: http://www.telegraph.co.uk/technology/3357777/Virgin-Media-blames-administrative-oversight-for-threats-on-warning-letters.html.
[65] *See e.g.:* Paul Ohm, *The Rise and fall of invasive ISP surveillance*, 2009 U. Ill. L. Rev. 1417 (2009); de Beer, Clemmer, op. cit. *supra* note 4; Chris Jay Hoofnagle, et. al., *Behavioral Advertising: The Offer You Cannot Refuse.*
[66] *See e.g.:* Hannibal Travis, *Opting out of the Internet in the United States and the European Union: Copyright, Safe Harbors, and International Law*, Notre Dame Law Review, Vol. 84, Issue 1 (November 2008), pp. 331-408.
[67] *See e.g.:* Timothy Wu, Copyright' s Communications Policy, 103 MICH. L. REV. 278, 279 (2004)

enforcement, without recognizing other important factors, could transform the Internet into a very different place.