



Master's thesis:

Combating copyright piracy in the EU: the application of Article 8 (3) of Directive 2001/29/EC against internet service providers

Subject area: European Intellectual Property Law & Policy in an International Context

Problem formulation: Internet service providers empower copyright piracy ecosystems by providing consumers with internet connectivity services. This study investigates the extent to which injunctions under Article 8 (3) of Directive 2001/29/EC may be used to compel internet service providers to combat copyright piracy and implement copyright enforcement measures online.

Name: Ivan Hadaya (vnh624)

Supervisor: Professor Timo Minssen, LL.D.

Number of characters: 137,211.

Date (Handing in): 27.6.2017

Can be published on the faculty of law library with grade:

Cannot be published on the faculty of law library:

Grade:

Table of content

1. Introduction	5
1.1 Background	5
1.2 Research questions	7
1.3 Delimitation	8
1.4 Methodology	9
1.5 Structure	9
2. Peer - to - peer file-sharing and copyright piracy: a technological preface	11
2.1 What is peer - to - peer file-sharing?	11
2.2 The evolution of peer - to - peer file-sharing technology	12
2.2.1 The Napster application: centralised file-sharing	12
2.2.2 BitTorrent technology: decentralised file-sharing	13
2.3 Streaming	14
2.4 Interim conclusions	15
3. Liability for copyright piracy	17
3.1 Who can be considered liable for copyright piracy?	17
3.1.1 End-users	17
3.1.2 Online sharing platform providers	18
3.1.3 Internet service providers	19
3.2 Interim conclusions	20
4. The EU legal framework applicable to copyright piracy and intermediary liability	21
4.1 Directive 2001/29/EC: the EUIPD	21
4.2 Directive 2000/31/EC: the eCommerce Directive	23

4.3 The Charter of Fundamental Rights of the European Union (2000/C364/01)	23
4.4 Interim conclusions	24
5. Internet service providers as involuntary copyright enforcers in the EU	26
5.1 CJEU considerations on the application of Article 8 (3) of Directive 2001/29/EC against internet service providers	26
5.1.1 <i>Promusicae</i> : subscriber information disclosure	26
5.1.2 <i>Scarlet Extended</i> : automated filtering systems	29
5.1.3 <i>UPC Telekabel Wien</i> : generic website blocking injunctions	31
5.1.4 <i>Filmspeler</i> : combating unlawful streaming services	34
5.1.5 <i>The Pirate Bay</i> : primary liability and torrent websites	36
5.2 Interim conclusions	39
6. Best practices and latest developments at the EU Member State level	41
6.1 Domestic application of Article 8 (3) of Directive 2001/29/EC against internet service providers.....	41
6.1.1 Sweden: <i>Swefilmer</i> as a landmark case	41
6.1.2 Denmark: Code of Conducts and one-stop-shop blocking	46
6.1.3 United Kingdom: live blocking orders as the forthcoming trend in the online copyright enforcement arena?	47
6.2 Interim conclusions	53
7. Analysis	55
7.1 Proportionality as key in determining the legality of injunctions under Article 8 (3) of Directive 2001/29/EC	55
7.1.1 Internet service providers as mere conduit intermediaries	56
7.1.2 The importance of balancing competing interests	56

7.1.3 Lessons learned from <i>Scarlet Extended</i> : Article 15 (1) of the eCommerce Directive and blanket monitoring	57
7.1.4 <i>UPC Telekabel Wien</i> : a targeted enforcement strategy contributes to proportionality	58
7.2 Criteria used for assessing proportionality of website blocking injunctions	60
7.2.1 Effectiveness	61
7.2.2 Substitutability	63
7.2.3 Availability of less restrictive alternative means	64
7.2.4 Implementation costs	65
7.2.5 Safeguards	66
7.3 Interim conclusions	66
8. Conclusion	68
Summary	71
Bibliography	73
Official Documents	73
Case law	74
Books	76
Articles	77
Websites	79

1. Introduction

1.1 Background

Copyright piracy (hereinafter ‘piracy’), commonly defined as the unauthorised copying and distribution of copyrighted content,¹ has been a legal problem that rights holders have struggled with for nearly two decades now,² and unprecedented amounts of piracy activities continue to occur on a daily basis around the world.³ The entertainment industry, in particular, has been affected by piracy, and rights holders have become worried about losing control over their exclusive economic rights, which are undermined by the unauthorised sharing of copyright protected content.⁴ For instance, according to a study released in 2016, the music industry in the EU endured a loss of approximately 170€ million in sales revenues as a consequence of the consumption of recorded music from unlawful sources.⁵ End-users, *i.e.* individuals surfing the web using computers, use file-sharing technology to share and obtain content (such as movies, music, software, and games) swiftly, and without having to pay for such content — and this is being done on a mass scale level.⁶ It was observed over 10 years ago that file-sharing technology has made popular media an easily available ‘public good’, without affording the authors of such works any economic remuneration.⁷ Although non-authorised exploitation of copyright protected content is ordinarily prohibited under national copyright law, and may give rise to criminal liability depending on jurisdiction,⁸

¹ L. Gelsthorpe, ‘Copyright infringement: a criminological perspective’, in J. Ginsburg (ed.), J. Davis (ed.), L. Bently (ed.), ‘Copyright and Piracy: an Interdisciplinary Critique’, Cambridge University Press Publishing, at 390 - 391 [2010]. In this study, the concepts ‘piracy’ and ‘unlawful file-sharing’ will be given the same meaning.

² J. Reyman, ‘The Rhetoric of Intellectual Property Law, Copyright Law and the Regulation of Digital Culture,’ Routledge, at 44 [2010].

³ B. Jütte, ‘The beginning of a (happy?) relationship: copyright and freedom of expression in Europe’, European Intellectual Property Review (hereinafter ‘E.I.P.R.’) 38(1), at 11 [2016].

⁴ S. Liebowitz, ‘The impact of internet piracy on sales and revenues of copyright owners,’ an abridged version of the full paper: ‘Internet piracy: the estimated impact on sales’, in Handbook on the Digital Creative Economy, Edited by R. Towse and C. Handke, Edward Elgar, at 35 [2013].

⁵ A study conducted by the European Union Intellectual Property Office, ‘The Economic Cost of IPR Infringement in the Recorded Music Industry,’ May 2016, at 5.

⁶ OFCOM, ‘Online copyright infringement tracker benchmark study Q3 2012: Introduction and Key Findings,’ at 3 [2012].

⁷ O. Pavlov, ‘Dynamic Analysis of an Institutional Conflict: Copyright Owners Against Online File Sharing,’ Journal of Economic Issues, v.39 (3), at 657 [2005].

⁸ N. Reich, ‘Understanding EU Law: Objectives, Principles and Methods of Community Law,’ Intersentia Publishing, at 166 [2005].

individuals are not always aware of the justifications of copyright protection, and it has been hard for the average consumer to regard consumption of popular media as theft or crime in the traditional sense.⁹

Copyright holders have tried to combat piracy by pursuing legal action against participants to the scheme at three different levels; the *content* level (websites and file-sharing applications), the *network* level (internet service providers), and the *end-user* level (individual end-user file-sharers). Some argue that copyright holders have failed in every single one of these levels, contending that the existing copyright enforcement measures are not fit to combat piracy, while others advocate increasingly stronger intellectual property rights (IPR) enforcement policies, contending that enforcement initiatives help mitigate piracy and protect their rights, never being quite satisfied with the level of protection afforded to them.¹⁰ Although successful legal action against copyright infringers has occurred in several Member States of the European Union (EU), rights holders have not been able to resolve the file-sharing problem as such, and it would seem that enforcing IPRs in the digital environment is becoming increasingly more challenging for rights holders all around the world.¹¹

This thesis investigates how rights holders can implement a proportionate and lawful copyright enforcement strategy against internet service providers (ISPs), *i.e.* those telecommunications companies which provide internet access and connectivity services to subscribers as their primary business function.¹² Targeting ISPs has become increasingly more commonplace among rights holders looking to combat piracy occurring online, and there are various reasons for why ‘ISP liability’ has emerged. The first reason has to do with that of ISPs *intermediary* position; they are situated at the nexus of internet communications between end-users (customers and non-customers) and the web, and are therefore able to implement wide-reaching enforcement measures with a view

⁹ T. Cvetkovski, ‘‘Copyright and Popular Media, Liberal Villains and Technological Change,’’ at 170 [2013].

¹⁰ P. Günther, ‘‘The plan for a digital Single Market in Europe and reforming EU copyright rules to develop a market-oriented approach to reduce infringement on the internet,’’ E.I.P.R. 38(1), at 45 [2016].

¹¹ A. Roy, A. Marsoof, ‘‘The blocking injunction: a comparative and critical review of the EU, Singaporean and Australian regimes,’’ E.I.P.R. 38(2), at 92 [2016].

¹² Notable examples of such ISPs include *Orange* (the Netherlands), *Telia* (Nordic countries), *Scarlet* (Belgium), and *Telefonica* (Spain).

to combat instances of piracy.¹³ Other reasons for the rise of ISP liability also exist; according to *Savola*, ISP obligations have emerged due to the following five reasons in particular:

- (1) ISPs have the capability to implement potent measures;
- (2) unlawful activities on the internet need to be tackled in some way, and previous measures have not been sufficient enough;
- (3) ISPs are vulnerable to new obligations;
- (4) ISPs need to take action due to public policy reasons; and,
- (5) ISPs may have private incentives to collaborate with rights holders.¹⁴

Giblin-Chen, on the other hand, argued long ago that rights holders will eventually shift their attention towards ISPs, primarily because tracking and chasing down individual end-users for unlawful file-sharing amounts to a “*teaspoon solution for an ocean problem*”.¹⁵ Both authors reasoning have merit, and due to ISPs capacity to implement potent measures in the information society, they have become increasingly more involved in the fight against piracy. Measures implemented by ISPs to safeguard copyright may be useful for rights holders looking to protect their copyright online, and the user-end website block, in particular, is currently trendy in the EU, and successful implementation has occurred in several EU Member States.¹⁶ As ISPs are able to implement measures which affect *all* their customers, it is no wonder that rights holders have shifted their attention from pursuing legal action against end-users and website operators to ISPs.

1.2 Research questions

This thesis will investigate the extent to which ISPs can be compelled to collaborate with rights holders in combating piracy websites. The following research questions will be investigated:

¹³ U. Kohl, “The rise and rise of online intermediaries in the governance of the Internet and beyond – connectivity intermediaries,” 26 IRLCT, at 193 and 200 [2012].

¹⁴ P. Savola, “Internet Connectivity Providers as Involuntary Copyright Enforcers: Blocking Websites in Particular,” University of Helsinki, Publications of IPR University Center, at 93 [2015].

¹⁵ R. Giblin-Chen, “Rewinding Sony: an inducement theory of secondary liability,” E.I.P.R. 27(11), at 429 [2005].

¹⁶ M. Schaefer, “ISP liability for blocking access to third-party infringing content”, E.I.P.R. 38(10), at 633 [2016]. User end-website blocking refers to a form of blocking where the ISP blocks access to a website from its own customers.

- (1) What is the role of ISPs in combating copyright piracy, and to what extent can measures under Article 8 (3) of the Directive 2001/29/EC be used to compel ISPs to enforce copyright online?
- (2) What proportionality considerations are of importance to keep in mind when looking to implement a lawful enforcement strategy under Article 8 (3) of the Directive 2001/29/EC?

The case law of the Court of Justice of the European Union (CJEU) is of nominal importance to the study, as several of its preliminary rulings serve to provide rights holders in the EU guidance on how to implement a lawful enforcement strategy under Article 8 (3) of Directive 2001/29/EC (the EU Information Society Directive, hereinafter ‘EUIDS’). Since Article 8 (3) does not come with objective guidance on its application, the CJEU has been the primary body of law which has provided for insight into what amounts to sound interpretation of the said EU law provision. The study leaves the case law of the European Court of Human Rights outside its scope for the most part, as the emphasis of this study is on the application of Article 8 (3) of the EUIDS.

1.3 Delimitation

Certain limitations to this study need to be established now. This study is concerned with injunctions against ISPs in particular, and will therefore not consider *direct* legal action against other parties engaging in piracy *per se*, like end-users and website operators.¹⁷ This restriction to the study is necessary for two reasons: first, considering direct enforcement against *all* liable parties for copyright infringement would require an analysis more exhaustive than what can be provided for within the procedural requirements of this thesis,¹⁸ and for this reason, it is necessary to restrict the subject-matter to enforcement against ISPs, as only then an in-depth discussion of the legal problem can be guaranteed; secondly, intermediary liability is presently a trendy subject in the digital copyright arena, and rights holders have increasingly shifted their attention away from suing end-users and websites to trying to transform ISPs in particular into ‘copyright enforcement officers’, who would do the hard work for them. To some extent, Article 8 (3) of the EUIDS has enabled for

¹⁷ A torrent website is a file-sharing website which facilitates piracy by indexing information pointing out to locations of unauthorised content. We will discuss torrent websites more in Section 2 of this study.

¹⁸ According to the University of Copenhagen rules, the master’s thesis must not exceed 140,400 characters in length.

this to happen, and ISPs in the EU have become increasingly more vulnerable to copyright enforcement mandates, as we shall see in this study. The outcome of this trend has been a higher level of IPR protection afforded to rights holders, but at the same time, new questions have emerged regarding especially the balancing of competing fundamental rights, and the threshold criteria to be used in determining the proportionality of measures against ISPs.¹⁹ An emphasis on EU law is present throughout the study, and for this reason, the significance of the case law of the CJEU is of nominal importance in answering the research questions. The study leaves the case law of the European Court of Human Rights outside its scope (for the most), as the emphasis of this study is on the application of Article 8 (3) of the EUIPD, in contrast to that of Human Rights Convention.

1.4 Methodology

The study methodology is legal doctrinal study. Legal sources will be used to develop ideas and construct discussion. The data used will consist of (1) *peer-reviewed academic articles* on copyright law and IPRs, (2) *books* relating to copyright law, (3) *case-law* from the Member State level as well as CJEU case law, (4) *legislation*, especially that of EU law, and (5) certain industry-relevant blogs and news portals (especially the *IpKat* and *TorrentFreak*), Peer-reviewed articles will have a more prominent influence to the study over books, as copyright law is a quickly evolving field of law, and therefore articles are better suited for providing food for thought regarding contemporary copyright issues, as books are like to become outdated rather quickly.

1.5 Structure

This study is compiled of eight chapters, structured with a view to provide for a logical whole capable of answering the research questions. We begin with the *introduction*, which establishes the research question, discusses the objective of the thesis, and sets out limitations to the study. Essentially, the introduction establishes the general outlook of the thesis and its content.

Second, we move on to a brief chapter on *file-sharing technology*. As this study adopts a ‘law & technology perspective’ in researching the legal problem, it is important that the technology aspect of the problem is addressed from a neutral point of view. This chapter is necessary to include in the

¹⁹ P. Letai, ‘Don’t think twice, it’s all right: toward a new copyright protection system’, E.I.P.R. 37(12), at 766 [2016].

study, as it is important to first understand the technical context in which infringements of copyright occur, before actually moving on to analyse the legal problems associated with such file-sharing technology.

Thirdly, a brief chapter on *copyright piracy and liability* is provided for, which discusses how different actors contribute to piracy ecosystems. In particular, this section will examine *how* piracy ecosystems are empowered by end-users, online platform providers, and ISPs.

Fourth, we highlights the applicable *EU legal framework* in relation to the subject-matter of the study, *i.e.* the EU laws, fundamental rights, and IPR principles which are of relevance to the study. As the study is primarily concerned with the application of Article 8 (3) of the EUIPD against ISPs, special emphasis will be given to the said Directive.

The fifth chapter will discuss the *role of ISPs as involuntary copyright enforcers*, and analyse the CJEU case law regarding especially the application of Article 8 (3) of the EUIPD. Ultimately, this chapter will enable us to start formulating the answer to the research questions.

The sixth chapter will discuss the latest *domestic developments* regarding ISPs and copyright piracy in Sweden, Denmark, and the United Kingdom. The countries have been chosen because they each provide for contemporary and interesting insight regarding the subject-matter of this study.

Using the previous two chapters as a basis, a seventh chapter — titled *analysis* — will be provided for, which will revolve around the *proportionality* of injunctions under Article 8 (3) of the EUIPD, and sum up the criteria that contribute to a proportionate enforcement strategy against ISPs, with particular focus on website blocking injunctions. This section will further make proposals relating to the proportionality of measures under Article 8 (3), as well as highlight what the future holds for rights holders looking to combat piracy through ISPs. Ultimately, this section of the study will enable us to answer the research questions posed in this study.

Finally, we will move to the actual *conclusion* — the eight chapter — which will address and answer the research questions. The introduction to the thesis is now set. The paper will proceed into a brief chapter on piracy and file-sharing technology, as it is important to examine the technology from a neutral perspective before moving on to address the legal problems surrounding it.

2. Peer - to - peer file-sharing and copyright piracy: a technological preface

2.1 What is peer - to - peer file-sharing?

As stated before, the study adopts a law & technology perspective, and so it is important to understand the technical aspects of file-sharing before moving on to legal problems. However, with a view to keep this study more legal than technical, the author will not get into the technicalities of file-sharing any more than what is necessary for us to examine the legal problems associated with file-sharing and piracy. Traditionally, when people speak of the internet, they think of the *World Wide Web*, which acts as a *centralised* server ‘platform’, where websites are stored and may be further accessed and browsed. However, peer - to - peer (P2P) networks function according to a different model: in P2P networks, each individual user who launches a P2P software and engages in P2P file-sharing schemes is called a *peer*,²⁰ whose computer not only becomes a server in the P2P network which can receive files from other peers, but also makes files stored locally available to other peers connected to the P2P network.²¹ This structure offers various advantages to peers: it lessens the burdens of individual servers, it enables the fast sharing of data, but also, owing to the *decentralised* nature of such P2P networks, the structure is relatively resistant to intervention by authorities and copyright holders. Consequently, P2P file-sharing has become a popular method to share and obtain copyright protected content without having to pay for such content, and copyright holders are deprived from obtaining remuneration for their works, as they are shared unlawfully without their consent.²²

Over a decade ago it was noted millions of people around the globe used P2P file-sharing technology,²³ and that P2P file-sharing networks amounted to more than 60% of *all* internet traffic taking place at any given moment.²⁴ In P2P networks, peers can share and obtain files among themselves, like music (eg. *Coldplay* albums), shows (eg. the *Game of Thrones* series) or software

²⁰ In this study, ‘peer’ will be used as a synonym to ‘end-user’.

²¹ M. Einhorn, ‘Media, Technology and Copyright: Integrating Law and Economics,’ Edgar Elgar Publishing Inc, at 79 [2004].

²² R. Haynes, ‘Media Rights and Intellectual Property,’ Capstone, at 3 [2005].

²³ K. Sideri, ‘The regulation of Peer-to-Peer Sharing Networks: Legal Convergence v. Perception Divergence’, in F. Macmillan (ed.), ‘New Directions in Copyright Law’, Edward Elgar Publishing Inc, at 216 [2005].

²⁴ H. Schulze and K. Mochalski, ‘Internet Study 2008/2009,’ Technical Report, Ipoque GmbH, [2009] in ‘EPFIA: Extensible P2P Flows Identification Architecture,’ Journal of Applied Mathematics and Physics, at 56 [2013].

(eg. the latest *Adobe Photoshop* software). Content shared can obviously be lawful, but it is commonly accepted that P2P file-sharing technology is being used on a mass scale to share illegal copies of copyright protected content. P2P networks remain to pose trouble to rights holders, and rights holders are constantly looking to create more stringent enforcement mandates to be implemented against the infringement of their copyright.

2.2 The evolution of peer - to peer file-sharing

P2P file-sharing technology has undergone constant technological evolution, making it increasingly more user-friendly, more efficient for its purposes, and ultimately, more litigation wary, as P2P online sharing platforms have, following various liability cases around the world, understood that they need to be careful with their actions, and refrain from making it seem that they provide services for the purposes of infringing copyright. As file-sharing technology is continuously evolving, rights holders constantly encounter new problems when looking to combat piracy. We will now move on to briefly examine the evolution of P2P file-sharing technology.

2.2.1 The Napster application: centralised file-sharing

P2P file-sharing first became the subject of legal discussion in the United States of America (USA) in the beginning of 21st century, where the file-sharing application *Napster* gained popularity like no other file-sharing application had ever before. Napster, which operated from 1999 to 2001, distorted the existing music markets of the time by introducing an application which allowed its users to share among themselves electronic copies of music (in MP3 form) without rights holders authorisation, and without affording remuneration to such rights holders. Due to the vast amounts of unlawful sharing activities taking place through the application, Napster was famously sued by the heavy-metal band Metallica for infringement of its exclusive rights, to which other artists in the musical industry later joined on.²⁵

²⁵ *A&M Records Inc v Napster, Inc*, 114 F. Supp 2d 896, U.S. District Court for the Northern District of California [2000]. By the time the legal proceedings commenced, Napster had already become very popular — at its peak, it had 80 million registered users. See: B. King, “The Day the Napster Died” [2002]. Available here: <https://www.wired.com/2002/05/the-day-the-napster-died/?currentPage=all> (accessed: 20.6.2017).

Due to the *centralised* nature of the application, which was freely available in Napster's website, Napster could monitor the data transfers taking place through their application.²⁶ Users interested in participating in Napster file-sharing had to download a software freely available in Napster's website, called *MusicShare*, and after installing it to their computers, users could use its search function to locate and download music files from other Napster users computers, as well as make available the content in their own computer to others.²⁷ Due to Napster's nexus position as an intermediary operating a centralised file-sharing application (having therefore the technical means to put an end to activities taking place through its servers), it became the subject of legal actions, which ultimately led the US Court of Appeals of the 9th Circuit to order Napster to terminate the operation and distribution of its software.²⁸

Since the days of Napster, P2P file-sharing technology has evolved. Not only has the popularity of P2P networks expanded from USA to the world, but the technology also has become more sophisticated, making it increasingly harder for rights holders to combat unlawful instances of copyright infringement via P2P file-sharing. Whereas the Napster application was centralised, directly pointing out to the individuals in charge of the networks, P2P networks are presently *decentralised*, meaning that they lack the kind of a supervisory operator as Napster was. Decentralised file-sharing marks the next significant advance in file-sharing technology, which will be considered now.

2.2.2 BitTorrent technology: decentralised file-sharing

After Napster, the next significant technological leap in the file-sharing arena was that of BitTorrent technology, introduced between 2003 - 2004. The *BitTorrent Protocol* is presently the most dominant P2P file-sharing network provider, and the technology is being widely used to distribute large quantities of unauthorised content.²⁹ The technology "chops" files into thousands of smaller pieces, so that pieces may be moved among several users in the network simultaneously and swiftly,

²⁶ Centralised file-sharing application require users to connect through the service providers own servers, and therefore the service provider assumes a supervisory position over the network.

²⁷ S. Stokes, "Digital Copyright, Law and Practice," Hart Publishing, at 133 [2005].

²⁸ *A&M Records, Inc. v. Napster, Inc.*, 284 F. 3d 1091, Court of Appeals, 9th Circuit [2002].

²⁹ Frontier Economics, "The Economic Impacts of Counterfeiting and Piracy: Report prepared for BASCAP and INTA," at 27 [2016]. According to BitTorrent official website, their protocols move as much as 40% of the internets daily traffic. See: <http://www.bittorrent.com/company/about> (accessed: 18.5.2017).

without being dependent on a central server to source the information.³⁰ This form of *decentralised* file-sharing has become very popular among end-users looking to engage in piracy, especially because it enables for the fast sharing of data, lessens the burdens placed on individual servers, and makes sharing unauthorised files hard police. To engage in BitTorrent file-sharing, a software implementing the BitTorrent Protocol needs to be used, like for example the popular *uTorrent* client.³¹ Once the client is installed, users can search torrent websites for torrents,³² which contain indexed lists of metadata, *i.e.* torrent files containing information regarding *where* (whose computer) a given file is located at. Once a torrent file has been found (eg. *Season 1 of Game of Thrones*), the user needs to launch it within the BitTorrent client (like uTorrent) in order to communicate with the various users holding pieces of the file pointed out in the torrent. Once this purely technical communication has been initiated, the end-user joins a *swarm*,³³ and begins to download the file from peers around the world, whilst simultaneously makes available pieces of the file available to other users, thus contributing to the general ecosystem of the P2P network.³⁴ This download/share aspect of BitTorrent is a crucial part of why the technology has become so popular — the more users engage in a swarm, the faster downloading becomes. Swarms are generally considered the part of BitTorrent file-sharing which gives rise to infringements of copyright.³⁵

2.3 Streaming

Streaming technology allows for the the transmission of multimedia over the internet, albeit not in the traditional way of downloading.³⁶ Streaming can be distinguished from downloading in that it

³⁰ B. Cohen, "The BitTorrent Protocol Specification," BitTorrent.org (Last modified February 4, 2017). <http://www.bittorrent.org/introduction.html> (accessed 20.6.2017).

³¹ Such applications are freely available online, and may be found simply by Googling "uTorrent" or "BitTorrent client".

³² *I.e.* metadata — a torrent contains information as to where a file is located at, but is not the file itself, and does not contain the file itself. The term derives from BitTorrent terminology.

³³ In BitTorrent terminology, a group of end-users who engage a BitTorrent file-sharing and share a certain file constitute a "swarm" in that given moment of sharing. When a user is part of a swarm, he not only downloads information from other peoples computers, but also shares the information simultaneously. The more end-users there are in a swarm, the faster the sharing of data is, as more servers interact among one-another.

³⁴ A. Stazi and D. Mula, "Intellectual Property and Consumer Law" in A. Ramalho (ed.), "Crossroads of Intellectual Property, Intersection of Intellectual Property and other Fields of Law," at 28 [2012].

³⁵ D. Kioupis, "Criminal Liability on the Internet", in I. Stamatoudi (ed.), "Copyright Enforcement and the Internet", Kluwer Law International Publishing, at 241 [2010].

³⁶ S. Stokes, "Digital Copyright: Law and Practice", Hart Publishing, at 157 [2009].

requires internet connection to access content, whereas torrenting (downloading via BitTorrent P2P) requires connection only initially. Streaming involves transiently accessing multimedia, whereas in torrenting, the file gets stored locally in the peers computer. Because torrenting involves copying material into the computer, it is generally perceived as more dangerous than streaming.³⁷ The streaming model of multimedia communications is increasingly more popular among end-users, which shows that end-users are not so much interested in *owning* content, but rather, they want to have *access* to content. Lawful streaming services generally allow for this, as content is not given to an end-user as such, but rather, the end-user receives access to content made available by authorised platforms. An example of such a lawful service is Netflix, which does not sell copies of movies and shows to individuals as such, but rather, is authorised by rights holders to make available content to its subscribers. While other success stories similar to Netflix exist, streaming technology has also become popular in piracy schemes, as it allows for streaming of popular media, and is generally perceived as being less dangerous than that of torrenting. However, as we shall see later on in the course of this study, the legal position unlawful streaming is becoming increasingly comparable to that of unlawful downloading, and the technical means to commit copyright infringement is losing relevance over other considerations, such as *intent* and *profit making*.³⁸

2.4 Interim conclusions

To sum this section up, P2P networks, which are *decentralised* and not supervised by any central authority, allow users to obtain copyright protected content stored in other peoples computers. Currently, the most popular way to engage in P2P file-sharing schemes is using the dominant *BitTorrent Protocol*, which has become a popular way for individuals to share unauthorised content. File-sharing technology itself cannot be considered *per se* illegal, as it is capable of substantial non-infringing uses,³⁹ but at the same time, actors contributing to the sharing of unlawful content cannot be admitted a complete free-pass merely because the technology used is capable of non-infringing

³⁷ “To torrent or to stream? That is the big piracy question.” TorrentFreak, May 29, 2017.

³⁸ Intent and profit making are especially noteworthy when addressing a websites extent of liability. The main sources of revenue for infringing web services are: advertising, subscription payments, payments per download, and voluntary donations. *See*: A joint project between Europol and the European Union Intellectual Property Office, “2017 Situation Report on Counterfeiting and Piracy in the European Union”, June 2017, at 31.

³⁹ *See*: Sony Corporation v. Universal City Studios, Inc., 464 U.S. 417 [1984]; the case provides for significant insight into the relevance of technology protecting doctrines.

uses.⁴⁰ Today, it is rather common knowledge that piracy prevails in P2P networks, and this is not controversial anymore.⁴¹

File-sharing technology is constantly evolving, posing new challenges to rights holders. In light of recent CJEU case law, which we will examine in later on in this study, unlawful streaming seems to slowly, but surely, become comparable to that of unlawful downloading, and the distinction in the technical means used to commit piracy is losing its relevance over other more relevant considerations.

⁴⁰ G. Mazziotti, “EU Digital Copyright Law and the End-User,” at 176 [2008].

⁴¹ As much has been accepted by Advocate General Maciej Szpunar in his recent Opinion in *Stichting Brein* (Case C-610/15), ECLI:EU:C:2017:99, at 23. Advocate General Maciej Szpunar recently advised the CJEU to rule that the piracy facilitating torrent website *The Pirate Bay* makes unlawful acts of communications to the public as portrayed in Article 3 (1) of the EUIPD, and he did so after accepting that *The Pirate Bay* facilitates data transfers of which 90% - 95% is unauthorised content.

3. Liability for copyright piracy

3.1 Who can be considered liable for copyright piracy?

To understand why ISPs have been pressured to collaborate with rights holders in combating unlawful file-sharing, it is important to understand the role of other parties contributing to piracy also. Essentially, actors contributing to piracy can be categorised into three parties: end-users, online sharing platform providers, and ISPs. We will now take a brief look at how these actors contribute to piracy.

3.1.1 End-users

End-users are the individual users participating in piracy schemes. They contribute to piracy ecosystems in many ways, by for example knowingly placing hyperlinks online giving access to unauthorised content, by operating online sharing platforms (eg. websites) facilitating unlawful file-sharing, by uploading infringing content to online platforms, or simply by sharing unauthorised content in P2P networks to others with a view to make available and obtain content for private use. Naturally, more potent measures are available against end-users who commit more severe copyright violations. However, in light of the amount of end-users engaging in piracy all around the world, targeting them is arguably a difficult, burdensome, and some would say, an *unfruitful* way of enforcing copyright in file-sharing cases. Reaping lawyers fees and compensation from such end-users after what can be several years of litigation is by no means guaranteed, and rights holders may end up assuming all costs themselves, although a finding of liability is *de jure* established. This is one reason why pursuing action against individual end-users is not the most preferable enforcement strategy for rights holders to take, unless the end-user in question is patently contributing to piracy ecosystems. Still, mass litigation and 'copyright trolling', *i.e.* pressuring end-users who have allegedly engaged in minimal amounts of infringing activities to pay settlement fees under the threat of litigation, does spark fear among the public, which *may* give rise to second thoughts to some individuals before engaging in pirate activities. Although this 'awareness effect' surely has a chilling and educational effect on some would-be infringers, the effect is not believed to be too significant, and instead, it would seem that fear-dominated policies have made the public more aware of the dangers of participating in piracy, and as a consequence, end-users have become

increasingly more sophisticated in doing so, using anonymity technology and online services to evade liability for copyright violations.⁴²

Targeting end-users does not seem to be a *sustainable* solution to combat file-sharing, and in light of the risk of being unable to recoup legal fees and compensation from individual end-users, it is submitted here that pursuing legal action against pirate end-users is advisable only when an end-user is significantly contributing to the functioning and availability of piracy ecosystems.

3.1.2 Online sharing platform providers

Online sharing platform provider is a relatively wide concept, which encompasses different kinds of service providers. In the piracy context, such platforms commonly take the form of torrent websites and server portals. Often, torrent websites are considered to be the primary wrongdoer contributing to P2P file-sharing. Direct action against torrent websites, as well as piracy application providers and streaming portal providers, *can* be a potent way to combat piracy, provided that operators of such websites can be identified and the individuals caught. There are many problems, however, when looking to target platform providers and operators directly. First of all, jurisdictional questions often arise in such cases, as platform operators may reside anywhere in the world, and piracy websites may be hosted overseas. Since piracy platform providers are often technically knowledgeable, they are also like to take technical measures to enhance their anonymity, and it takes a lot of resources for rights holders to chase such individuals. Further, catching the operators themselves does not necessarily mean that the platform will stop from functioning, as spinoff version of platforms may be created by other copyright pirates. This has become apparent especially from the Swedish originating *The Pirate Bay (TPB)* saga, where the local courts ruled against the original operators of torrent website⁴³ — a judgement whose lawfulness has been affirmed by the European Court of Human Rights⁴⁴ — but still, although the website has been ordered to stop functioning on many instances, the legacy of The Pirate Bay continues to live, and TPB proxy

⁴² P. Günther, M. Norrgård, “Blocking Websites: Copyright Enforcement Online and Responsibilities of Internet Intermediaries in Europe”, JFT 3/2014, at 131 [2014].

⁴³ Stockholm's District Court (*Tingsrätt*) ruling in case B 13301-06.

⁴⁴ ECHR Decision of the ECtHR (5th section) of 19 February 2013. Case of Fredrik Neij and Peter Sunde Kolmisoppi (The Pirate Bay) v. Sweden, Appl. nr. 40397/12; ECLI:CE:ECHR:2013:0219DEC004039712.

websites are still available and widely being used by end-users around the world to search and download unauthorised content.

Like in the case of targeting end-users, there is no guarantee that online sharing platform operators have the financial means to compensate the significant damages they are like to be ordered to pay rights holders, and for this reason, it is risky for rights holders to use resources and time to pursue legal action against such platform providers. Although legal action against hosting providers may be taken with a view to compel such hosting providers to stop hosting given websites, it has become apparent that this strategy leads bad faith website operators to simply register with another hosting provider, often overseas in strategically located jurisdictions. Due to the jurisdictional problems associated with targeting website operators directly, and the fact that such operators often remain anonymous and are hosted overseas, it is understandable why rights holders have increasingly shifted their attention from targeting such online sharing platform actors to targeting ISPs.

3.1.3 Internet service providers

ISPs, often dubbed as the 'gate-keepers' of the internet,⁴⁵ provide internet access to consumers as their main function as a business entity. They therefore *empower* any copyright infringing activities conducted by their customers, albeit without doing so intentionally. ISPs also host websites, and such websites may contribute to unlawful file-sharing. This nexus position in which ISPs are at has placed them under legal pressure: rights holders have argued that, because ISPs services are being used to infringe copyright, they should play a more active role in combating piracy, by for example blocking access to infringing websites and disclosing subscriber information. Often, copyright holders have further argued that ISPs should be themselves responsible for assuming costs associated with implementing measures to protect copyright, as it is by virtue of their services that end-users are able to partake in piracy in the first place. Whether holding ISPs solely responsible for implementation costs which are designed to protect rights holders copyright is reasonable or not is a matter yet to be resolved at the EU level, but generally, Member States have ordered ISPs to assume implementation costs themselves. Intimidated by implementation costs and enforcement mandates, ISPs have sought refuge from liability and enforcement mandates by arguing that they have a right

⁴⁵ H. K. Larusson, "Uncertainty in the scope of copyright: the case of illegal file-sharing in the UK," E.I.P.R. 31(3), at 130 [2009].

to conduct a business as portrayed in Article 16 of the EU Charter, and that they do not intentionally further any infringing activities by their customers, but rather act as 'mere conduit providers' as regulated in the Directive 2000/31/EC (eCommerce Directive). Simultaneously, they have argued that they have an obligation to protect the private and family life of their customers, as well as contribute to protecting the data of their customers.

Nevertheless, rights holders in Europe have been relatively successful in compelling ISPs to collaborate with them in combating unlawful file-sharing. Under EU copyright law, ISPs are subject to injunctions by way of Article 8 (3) of the EUIPD, which provides that Member States need to make sure that copyright holders may obtain injunctive relief from intermediaries whose services are being used by third-parties to infringe copyright. Although initially there existed controversy over whether Article 8 (3) could be applied against ISPs, it has been by now confirmed by the CJEU on many instances that such ISPs must be regarded as 'intermediaries' within the meaning of Article 8 (3).⁴⁶ As the CJEU has confirmed that ISPs qualify as intermediaries in this context, rights holders in the EU should, in theory, always be able to apply for injunctions against ISPs, with a view to obtain injunctive relief from infringements conducted by subscribers of ISPs.

3.2 Interim conclusions

We have considered the extent to which end-users, online sharing platform providers, and ISPs empower piracy ecosystems. It was noted that rights holders have increasingly shifted their attention towards ISPs, as ISPs can implement wide-reaching measures against both end-users and online platform providers. It was also noted that pursuing legal action against end-users and online platform providers is arguably difficult, and rights holders may encounter especially jurisdictional problems when looking to implement their copyright enforcement strategy against such actors. Hereinafter we will only consider end-users and online sharing platform providers only to the extent that they are relevant to the subject-matter of this thesis, *i.e.* ISP enforcement obligations.

⁴⁶ C-557/07, LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH, at 46 [2009].

4. The EU legal framework applicable to copyright piracy and intermediary liability

As copyright is generally a territorial right, no harmonised copyright law *per se* exists in the EU. Copyright directives, however, do establish minimum requirements and standards, which Member States need to adhere to within their respective jurisdictions. Two directives are particularly important for the purposes of this study; the *EUISD*⁴⁷ and the *eCommerce Directive*.⁴⁸ Although the *IP Enforcement Directive*⁴⁹ is also noteworthy in the context of IPR enforcement matters, it is explicitly provided in the IP Enforcement Directive that its provisions apply *without prejudice* to the enforcement provisions of the EUISD, and in particular, that of Article 8.⁵⁰ Therefore, so far as matters covered by Article 8 (3) are concerned, that provision takes precedence over the provisions established by the IP Enforcement Directive.⁵¹ However, it is good to note that, in any event, the injunction provisions provided by both the EUISD and the IP Enforcement Directive are very similar, the main difference being that the IP Enforcement Directive is applicable to other civil IP enforcement matters, like patent and trademark litigation, whereas the EUISD applies to matters of copyright and related rights.

4.1 Directive 2001/29/EC: the EUISD

The EUISD concerns the legal protection of copyright and related rights in the information society.⁵² Among other things, the directive enshrines international copyright obligations that the EU has committed to,⁵³ and seeks to make sure that adequate legal protection of copyright in the digital environment is secured in the Member States of the EU. The Directive also touches upon intermediary liability, as it acknowledges that sometimes intermediaries are best placed to put an

⁴⁷ 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.

⁴⁸ 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.

⁴⁹ Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

⁵⁰ *Id.*, Article 2 (2) as well as Article 11.

⁵¹ For a wide overview of the application of the IP Enforcement Directive, *see*: G. Cumming, M. Freudenthal, R. Janal, "Enforcement of Intellectual Property Rights in Dutch, English and German Civil Courts", Kluwer Law International Publishing [2008].

⁵² Article 1 of the EUISD.

⁵³ Namely, the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty, which have been made reference to in Recital 15 of the Directive.

end to infringing activities.⁵⁴ Importantly, the Directive requires Member States to put into place sanctions and remedies for infringements of rights and obligations as set out in the directive.⁵⁵

Article 2 of the EUIDS provides for the *reproduction right*, which requires Member States to make sure that rights holders (who are defined under Article 2 (a) - (e) of the Directive) have the exclusive right to authorise and or prohibit other parties from reproducing their protect content. Article 3 (1) provides for the *communication to the public* right, which requires Member States to make sure that authors have the exclusive right to authorise or prohibit the communication of their protected works. This provision is of pivotal importance to the EU copyright arena,⁵⁶ and further attention will be paid to Article 3 (1) as we move on with the study. Article 5 (1) — a provision that has been interpreted rather strictly by the CJEU⁵⁷ — affords intermediaries some shield from liability. It provides that intermediaries are exempted from the reproduction right contained in Article 2, provided that the act in question is temporary, transient or incidental, an integral and essential part of a technological process, the sole purpose of which is to enable transmission in a network between third parties by an intermediary or a lawful use of a work, and which does not have any independent economic significance. For the purposes of this study, however, the most significant provision in the Directive is Article 8 (3), which provides that:

“Member States shall ensure that rights holders 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.”

This provision is of pivotal importance to our study, as it has been used by rights holders to pave the way for ISP obligations in the piracy context. Article 8 (3) does not provide for any guidance on its correct application, but merely requires Member States to enable rights holders to apply for injunctive relief. As is common with EU directives, implementation is left to Member States, and

⁵⁴ Recital 59 of the EUIDS.

⁵⁵ Recital 58 of the EUIDS.

⁵⁶ For a brief but good paper on the notion of “communication to the public” in the EU, see: Dr. Clark, S. Tozzi, “Communication to the public under EU copyright law: an increasingly Delphic concept or intentional fragmentation?”, E.I.P.R. 38(12), 715-717 (2016). Note that the paper does not take into account of the recent case handed down by the CJEU in *Filmpeleer*, which will be discussed further in Section 5 of this study.

⁵⁷ See: Infopaq International (ECLI:EU:C:2009:465) for in-depth analysis of the application of Article 5 (1) of the EUIDS.

for this reason, the CJEU considerations and constraints on the application of injunctions under Article 8 (3) are of nominal importance to us.

4.2 Directive 2000/31/EC: the eCommerce Directive

The *eCommerce Directive* seeks to, *inter alia*, ensure the free movement of information society services within the European Union.⁵⁸ Importantly, to our file-sharing problem, the Directive establishes provisions on exemptions to intermediary liability for infringements happening in the information society. Under the eCommerce Directive, an information society service provider may benefit from an exemption regime, provided that it satisfies the requirements set in Articles 12 - 14 of the Directive. Articles 12 - 14 of the Directive provide for the provisions creating the so-called *safe harbor* regime, *i.e.* the Directive's liability exemption regime. However, according to Recital 45 of the Directive, the exemption regime does not preclude the possibility of issuing injunctions against service providers, and for this reason, the relevance of exemption regime is not too significant to our research. Article 15 of the Directive, however, prohibits Member States from requiring service providers to conduct *general monitoring* of their networks, and this is of importance to our research. In the file-sharing context, Article 15 has been very significant in that it has been used to *challenge* rights holders enforcement attempts, and in some cases, the said provision has rendered enforcement attempts disproportionate and unlawful.⁵⁹ Although Article 15 of the eCommerce Directive has been significant in limiting rights holders enforcement requests from becoming disproportionate, the rest of the eCommerce Directive has been relatively inapplicable to ISP liability in the piracy context. The safe-harbour regime affirms that ISPs cannot be held primarily liable for their customers infringing activities, but at the same, it does not preclude the application of injunctions against such ISPs.

4.3 The Charter of Fundamental Rights of the European Union (2000/C364/01)

The *EU Charter* is a document at the very heart of EU law, which establishes the fundamental rights that are protected in the EU.⁶⁰ The relevance of fundamental rights in Europe is constantly

⁵⁸ As much is stated in Recital 8 and Article 1 (1) of the eCommerce Directive.

⁵⁹ *Scarlet Extended SA v SABAM* (Case C-70/10); the case will be discussed in greater detail later in the study.

⁶⁰ The Charter of Fundamental Rights of the European Union (2000/C364/01).

increasing, and the role of fundamental rights within the EU IPR framework is a matter which, although has been researched, is still open for exploration.⁶¹ The EU Charter itself regulates various types of matters: *inter alia*, it prohibits torture, enshrines the right to conduct a business, and requires that intellectual property shall be protected.⁶² Since the entry into force of the Treaty of Lisbon in 2009, the Charter has been directly applicable as such to Member States of the EU.

In injunction cases against ISPs, the most relevant provisions in the Charter are the following: the right to *respect for private and family life* (Article 7); the right to *protection of personal data* (Article 8); *freedom of expression and information* (Article 11); *freedom to conduct a business* (Article 16); the *right to property and protection of intellectual property* (Article 17); and the right to an *effective remedy* (Article 47). In addition to the previously mentioned provision, Article 52 (1) is important in highlighting the importance of the principle of proportionality in cases where fundamental rights are limited. Indeed, the *principle of proportionality* has been of nominal importance in the CJEU case law, and this is true also regarding the application of Article 8 (3) of the EUIPD against ISPs. The CJEU has recurrently stated that the enforcement strategies copyright holders pursue must be *balanced* with other affected rights. The question of conflicting fundamental rights and their balancing is a very relevant concern that rights holders need to keep in mind when planning their copyright enforcement strategies, as disproportionate enforcement strategies are like to be challenged on such grounds, and ultimately declared unlawful or rejected by the courts.

4.4 Interim conclusions

We have examined the relevant EU laws applicable to the research problem. It was noted that no absolute harmonisation of copyright law exists in the EU, but rather, the Member States are bound by various copyright directives, which require them to make sure a certain level of copyright protection to be granted to rights holders within their respective jurisdictions. The EUIPD, together with its Article 8 (3), is of pivotal importance to our study, as we are specifically concerned with enforcement against such ISPs in the piracy context. The role of the eCommerce Directive has been relatively minimal, with the exception of its Article 15, which has had a limiting effect on

⁶¹ J. Griffiths, L. McDonagh, “Fundamental Rights and European IP law: the case of Art 17 (2) of the EU Charter”, in C. Geiger (ed.), “Constructing European Intellectual Property: Achievements and New Perspectives,” European Intellectual Property Institutes Network series, at 75-76 [2013].

⁶² EU Charter, Articles 4, 16, and 17 (2).

enforcement measures to be implemented against ISPs, as we shall see in the following chapter of this study. We will move on to examine CJEU case law on file-sharing, with a view to examine the application of Article 8 (3) of the EUIDS against ISPs, and the extent to which ISPs may be compelled to collaborate with rights holders in enforcing copyright online under EU law.

5. Internet service providers as copyright enforcers in the EU

5.1 CJEU considerations on the application of Article 8 (3) of the EUIPD against internet service providers

ISP liability is a controversial legal topic, and many challenges lie ahead.⁶³ Following the difficulties national courts have had with interpreting the relevant EU laws and applying them in file-sharing cases, the CJEU has been asked to elaborate upon the legal position of ISPs when their services are used by third-parties to engage in piracy. We will move on to examine the relevant rulings of the CJEU, with a view to begin formulating an answer to the research questions posed earlier in this study.

5.1.1 *Promusicae*: subscriber information disclosure

Data protection and privacy is afforded a high level of protection in the EU, and for this reason, the question of converting internet protocol addresses (IP address) into personal data has been problematic.⁶⁴ In the digital space, a computer is identified by its IP address, which is a set of numbers given by the ISP to its subscriber. An IP address points out the specific ISP who has assigned the identification code to its customer, and ISPs can convert an IP address into personal data such as names and addresses, which reveal their customers identity. Simply Googling an IP address discloses the ISP empowering it, but only ISPs can convert the number series into personal data indicating who the end-user is. Rights holders monitor unauthorised transfers of their content in infringing P2P platforms, usually by hiring a specialised technical company to do so, and once they have collected IP addresses infringing their copyright, by for example monitoring BitTorrent swarms, they forward the evidence to locally based lawyers, who request the court for an order compelling ISPs to convert the IP address into personal data indicating the individual from whose internet connection account the infringements were done. Despite the fact that subscriber information disclosure is relatively controversial still today in 2017, it has been successfully used

⁶³ P. Akester, "The new challenges of striking the right balance between copyright protection and access to knowledge, information and culture," E.I.P.R. 32(8) at 373 [2010].

⁶⁴ In addition to Articles 7 and 8 of the EU Charter, the Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector also regulates the processing of personal data.

over the years in the following EU Member States at least: Finland, Germany, France, The Netherlands, Austria, Sweden, Denmark, and the UK.⁶⁵

ISPs, on the other hand, have the obligation to, *inter alia*, protect their customers personal data, and process it in a manner compliant with data protection laws. In the case of subscriber information disclosure, the protection of data and privacy conflicts directly with the protection of IPRs, both which are portrayed as fundamental rights under the EU Charter. ISPs have been generally reluctant disclose their users personal data, not because of their disregard to the protection of IPRs, but instead, because they have been worried about becoming burdened by copyright holders enforcement requests, of violating consumers fundamental rights, of becoming less appealing to consumers, and of being required to assume enforcement related implementation costs. This conflict became apparent *Promusicae*,⁶⁶ a case which initially started in Spain, but was ultimately considered by the European Court of Justice (ECJ), now part of the CJEU. Promusicae was a non-profit organisation operating in Spain and dealing with the protection of its members copyright and related rights in musical works. In 2005, Promusicae sued Telefonica (an ISP), contending that it wanted the ISP to convert a series of IP addresses into personal data for the purposes of enabling it to pursue legal action against the anonymous customers of Telefonica, who, Promusicae contended, had been participating in unlawful file-sharing activities via the P2P file-sharing application known as KaZaA. Telefonica refused to collaborate with Promusicae, arguing that EU law did not require it to do so, and that EU data protection law only permitted disclosing such personal information in cases which had a criminal law aspect to it, or where national security was under a real threat. The Commercial Court in Madrid⁶⁷ referred the case to the ECJ for a preliminary ruling, asking whether, in light of various EU laws,⁶⁸ Member States could order ISPs to convert IP addresses into personal

⁶⁵ See European Commission, ‘‘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,’’ SEC(2010) 1589 final, at 12–13. For an analysis of the European situation on subscriber information disclosure, see generally: *See generally*: M. Daly, ‘‘Is there an entitlement to anonymity? A European and international analysis’’, E.I.P.R., 35(4), 198 - 211 [2013].

⁶⁶ Case C-275/06, *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU*, Judgment of the Court (Grand Chamber), 29 January 2008.

⁶⁷ The Juzgado de lo Mercantil No 5 de Madrid.

⁶⁸ The EU Charter (2000/C 364/01); eCommerce Directive (2000/31/EC); IP Enforcement Directive (2004/48/EC); EUISD (2001/29/EC).

data indicating the identity of individuals for the purposes of enabling rights holders to pursue civil proceedings against such alleged infringers of copyright.

The ECJ issued its preliminary ruling in 2008. In the ruling, the ECJ provided that there was nothing in the *ePrivacy Directive*⁶⁹ which did not allow for Member States to regulate that internet traffic data could be disclosed for the objective of providing rights holders the potential to take civil action against copyright infringers. Simultaneously, however, the court noted that there was no provision under EU law which compelled Member States to permit such a possibility to rights holders. Instead, the ECJ provided that it was for Member States to implement the various data protection and copyright laws under their own discretion, in a manner which is *fair and proportionate*, successfully balancing the conflicting fundamental rights that are relevant in the issue.⁷⁰ The ruling highlights that, so long as competing fundamental interests are balanced, EU law does not preclude Member States from introducing regulations to compel ISPs to convert IP addresses into identity-disclosing data for the purposes of enabling rights holders to pursue legal action against them, but at the same, Member States are not directly compelled by EU law to provide for such a possibility to rights holders. The ECJ left it for authorities in Spain to decide on how to proceed with the matter.

Some authors have argued that the *Promusicae* ruling has "tipped" more in favour of IPR holders than what the EU perhaps intended to do,⁷¹ as following the ruling, it has been affirmed that Member States may allow for the conversion of IP addresses into personal data for the purposes of enabling rights holders to pursue civil suits against alleged copyright pirates. Unfortunately, the ECJ itself did not elaborate on what constitutes proportionate implementation of the matter, and this question is open for interpretation still today. However, it is submitted that the *de minimis* principle can be useful to rights holders, and that pursuing action against non-recurring end-users who have engaged in insignificant amounts of file-sharing activities is not advisable; in contrast to this, the need to protect IPRs (and hence the need for the information disclosure order) is more significant

⁶⁹ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

⁷⁰ Case C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, Judgment of the Court (Grand Chamber), at 70 (2008).

⁷¹ Joel Smith, "European Community: copyright - data privacy does not trump copyright protection," *E.I.P.R.* 30(6) N39, at N39 [2008].

when targeting end-users who contribute patently to piracy ecosystems. It is proposed here that rights holders focus on such individuals, as the chances of receiving an information disclosure order is greater when rights holders can show the court that the need for such an order is pressing in light of the severity of the infringements, in contrast to being merely symbolic and amounting to copyright trolling.

5.1.2 Scarlet Extended: automated filtering systems

Filtering technology has been addressed by the ECJ in *Scarlet v SABAM*,⁷² the former being an ISP, the latter a collecting society concerned with protecting its members copyright. Here, a filter refers to an infringement detector system, implemented by the ISP, designed to prevent its subscribers from using the ISP's services to participate in unlawful file-sharing activities or any other mode of piracy. In 2004, SABAM sued Scarlet in the Belgian High Court, with a view to compel Scarlet to implement a filter which would supposedly stop its customers from participating in file-sharing activities which violated SABAM's copyright. The court accepted SABAM's claim that Scarlet's customers were participating in copyright infringing activities, and further affirmed that Scarlet should make an effort to stop its customers from participating in piracy. However, before moving on to order Scarlet to implement such a filter, the court asked a technical expert to investigate whether such a filter would be effective for its purposes. The technical expert conducted research on the matter for three years, and in 2007, he concluded his report: out of the 11 technical solutions that he investigated for the court's purposes, he considered that only one might be able to achieve the court's objective, and that even that solution was imperfect and would be costly to implement. SABAM nevertheless succeeded in convincing the court that the solution should be adopted and implemented, and the court ruled that Scarlet was to implement the filter within 6 months time.

The filter sought by SABAM was very extensive by nature: (1) it was to apply to all of Scarlet's traffic; (2) to all of its customers; (3) for an unlimited amount of time; (4) as a preventive mechanism; and (5) exclusively at the expense of the ISP.⁷³ While Scarlet did try to implement the filter, it found itself facing various technical problems in doing so. It requested the court to consider

⁷² Case C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, (2011), Judgment of the Court (Third Chamber).

⁷³ *Id.*, at 29.

the matter again, and after the court refused to change its stance on the matter, Scarlet appealed the decision to the Belgian Court of Appeal, contending that implementing such a filter would amount to general surveillance of its networks as prohibited by Article 15 of the eCommerce Directive, and that such filtering involved processing personal data of its customers in a manner which was in breach of EU data protection law.⁷⁴ The Belgian Court of Appeals referred the case together with accompanying questions to the CJEU for a preliminary ruling on the matter. In particular, it sought to ask whether such a filter was lawful under the various EU laws applicable. The ECJ issued its preliminary ruling in November 2011.

The ECJ noted that precedent EU law provided that injunctions could be issued against service provider intermediaries for the purposes of protecting rights holders IPRs, and while it affirmed that injunctions could be granted against ISPs, it noted that the injunction SABAM sought was particularly wide-reaching, and that implementing such a filter would be disproportionate as it would require general monitoring of its customers which would be in breach of EU privacy and data protection law, and in particular, in breach of Article 15 of the eCommerce Directive.⁷⁵ Having ruled that such a filter breached EU privacy and data protection law, the Court concluded that the injunction sought by SABAM failed to strike an appropriate balance between the conflicting fundamental rights at stake, namely, the ISP right to conduct a business and consumers' right to privacy as secured in the Privacy Directive and the EU Charter.⁷⁶ Consequently, Scarlet was relieved from implementing the injunction.

The preliminary ruling is important in that it makes clear that there exists the possibility of using injunctions against ISPs with a view to compel them to enforcement measures, but such measures must not disproportionately collide with other fundamental rights, and must be proportionate and suitable for its purposes. Thus, proportionality considerations are of paramount importance when considering how to implement copyright enforcement strategy, as the lack of proportionality from the side of rights holders can be pivotal in rendering the whole enforcement strategy unlawful. There are many considerations that proportionality evaluation should take into account, like

⁷⁴ Id, at 26.

⁷⁵ Id, at 39 - 40.

⁷⁶ Id, at 53 - 54.

whether there exists alternative less restrictive means, or in the context of filtering technology, whether such filters deprive individuals from being able to obtain material for fair use. SABAM was forced to surrender its case, and although this has been the leading case with regard to filtering technology in the file-sharing context within the EU, this does not mean that a more *modest* filter-request cannot be considered in the future: ‘*filtering is not dead, it’s just resting*’.⁷⁷

5.1.3 UPC Telekabel Wien: generic website blocking injunctions

ISPs have the technical capacity to block access to websites. User-end website blocking occurs when an ISP blocks its customers from being able to reach a website. In the EU, website blocking has been achieved by way of *injunctions* — a potent enforcement tool — which can be beneficial to rights holders, allowing for them to obtain injunctive relief from infringements of their rights. Website blocking is currently an increasingly more trendy strategy taken by copyright holders to combat piracy, but although a potent way to combat piracy, such blocks are not perfect as such, and may be bypassed by informed internet users.⁷⁸ Nevertheless, although website blocking is not perfect, it is nowhere stipulated that enforcement measures must be perfect and absolute, and the fact that rights holders have been motivated to make ISP implement such blocks goes to show that such blocking has significance to rights holders.

In the EU, ISPs have been compelled by courts to implement blocking against piracy facilitating websites. In some countries, using blocking injunctions to combat piracy has been common practice for several years now, whereas in other countries, no such block has yet been issued, or only just very recently.⁷⁹ ISPs have often been reluctant to implement enforcement mandates that rights holders have come up with, stressing their position as mere conduit providers, and arguing that

⁷⁷ D. Meale, ‘SABAM v Scarlet: of course blanket filtering of the internet is unlawful, but this isn’t the end of the story,’ E.I.P.R. 34(7), at 431 [2012].

⁷⁸ Technical means allowing for circumvention of ISP implemented blocks are available, like for example Virtual Private Networks (VPNs) and proxy services.

⁷⁹ For example, in Sweden, the first user-end website block against a piracy website was granted in February 2017. We will take a look at this case in the following chapter of this study.

compelling them to implement measures to protect rights holders copyright hinders their right to conduct a business as portrayed in Article 16 of the EU Charter.⁸⁰

Injunctions requiring ISPs to implement blocking measures was a matter notably examined by the CJEU in *UPC Telekabel Wien*,⁸¹ where the CJEU ruled that a *generic* blocking injunction, *i.e.* a blocking request made by rights holders in a general form, is acceptable in relation to ISPs right to conduct a business. Such generic requests to block a website afford ISPs a certain amount of discretion, as it is left to the ISPs to decide how to achieve the block. The CJEU effectively confirmed that ISPs stand in a very pivotal position in the piracy problem, and that they may be consequently required to take measures to protect rights holders copyright when their services have been used by third-parties to take part in unlawful file-sharing activities online. Blocks, the CJEU provided, must be effective, and they must strike a balance between the rights that conflict which each other, *i.e.* the interests of the rights holders, ISPs, consumers, and website operators. ISPs must take "*all reasonable measures*" when considering how to implement a blocking injunction in practice, and at the same time, they must not unnecessarily deprive their customers from being able to take part in lawful activities and access lawful content.⁸² We will now examine the facts of this important case in more detail.

The dispute first emerged in Austria, where Wega (rights holder) asked UPC (ISP) to block access from its customers to the German streaming and torrent website *kino.to*, as the website had been shown to facilitate the sharing of Wega's copyright protected content (films). Wega was concerned about its exclusive rights being distributed through *kino.to* without its consent, and requested the domestic court to issue an injunction ordering UPC to block access to *kino.to* from its users. The Austrian Court ruled that UPC acted as an intermediary who empowered its customers pirate activities, and went on to grant Wega the injunction it sought.

⁸⁰ See generally: K. T. O'Sullivan, "Enforcing copyright online: internet service provider obligations and the European Charter of Human Rights", E.I.P.R. [2014]. In the paper, the author argues that Article 16 of the EU Charter only plays a limited role when the issue in stake is that of protecting rights holders intellectual property.

⁸¹ Case C-314/12, *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH*, (2014).

⁸² *Id.*, at 42 and 64.

UPC challenged the decision, arguing that the blocking injunction was not in conformity with EU law, and ultimately went on to appeal the decision to the Supreme Court of Austria. The Supreme Court then referred the case to the CJEU, and asked:

‘‘Is Article 8(3) of Directive 2001/29 ... to be interpreted as meaning that a person who makes protected subject-matter available on the internet without the right holder’s consent [for the purpose of Article 3(2) of Directive 2001/29] is using the services of the [internet] access providers of persons seeking access to that protected subject-matter?’’⁸³

The CJEU answered that Article 8 (3) of the EUISD should be interpreted as meaning that where a person makes copyright protected content available to the public, and without permission of the rights holder, that person is using the services provided by the ISP for unlawful purposes, making the ISP an intermediary subject to injunctions within the meaning of Article 8 (3), and further, that EU fundamental rights do not preclude courts from issuing generic orders prohibiting ISPs from allowing consumers to access websites placing protected content online without permission of the rights holders, subject to two conditions:

- (1) the measures taken cannot unnecessarily deprive internet users of the possibility of lawfully accessing the information available; and,
- (2) those measures must prevent unauthorised access to the protected content, or at least seriously discourage consumers from doing so.⁸⁴

Following the ruling, it has become clear that, under the EU legal framework, ISPs may be compelled to collaborate with rights holders in combating piracy empowered by their services. This is certainly good news for rights holders, as following the ruling, copyright holders may now generally ask ISPs to block patently infringing websites from their customers reach, given that the request is proportionate, and based on legally sound merits. It has been left for ISPs to decide on how they will achieve such blocks, and they will need to take *“all reasonable measures”* in order to avoid a further finding of liability from their side, as well as satisfy the above to requirements. The

⁸³ Id, at 17.

⁸⁴ Id, at 64.

CJEU, unfortunately, refrained from providing a more in-detail description of the meaning of "all reasonable measures", and left this for Member States (and ultimately ISPs) to resolve.

5.1.4 *Filmspeler*: combating unlawful streaming

On the 26 April 2017, the CJEU handed down its long awaited decision in *Filmspeler*,⁸⁵ where it ruled that selling a multimedia player configured to provide access to unauthorised multimedia amounts to communication to the public within the meaning of Article 3 (1) of the EUISD. Although the preliminary ruling does not concern Article 8 (3) of the EUISD and ISPs as such, it has implications on ISPs copyright enforcement in the EU, and will consequently be discussed.

The case originated from The Netherlands, where the Dutch anti-piracy organisation Stichting Brein sued Mr. Wullems for selling various models of multimedia players (named Filmspeler) to consumers under his website www.filmspeler.nl. The multimedia players functioned as a medium between internet and television, whereby by utilising the availability of streaming websites not created by Filmspeler itself, the player could (when connected to the internet) retrieve sound and images from streaming websites, and transmit them into a television. The Filmspeler multimedia player had a user-friendly interface, and contained pre-installed 'add-ons' created by third-parties, which users could click to stream multimedia content like films widely sourced from third-party copyright infringing streaming websites. After initially asking Mr. Wullems to stop selling the multimedia player, Stichting Brein sued him in the District Court of Central Netherlands for copyright infringement, arguing that he was communicating unauthorised works to the public, in violation of the Article 13a of the Netherlands Law on Copyright (*Auteurswet*), which implemented Article 3 (1) of the EUISD. Stichting Brein applied for an injunction against Mr. Wullems, ordering him to stop selling his Filmspeler multimedia players, and stop offering hyperlinks that enabled users to access unauthorised content and protected works.⁸⁶

The District Court referred questions to the CJEU, asking, *inter alia*, whether the sale of the multimedia players amounted to communication to the public within the meaning of Article 3 (1) of

⁸⁵ Judgement of the Court (Second Chamber) of 26 April 2017, *Stichting Brein v Jack Frederik Wullems*; ECLI:EU:C:2017:300 (2017).

⁸⁶ *Id.*, at 19.

the EUIPD. The CJEU noted that Mr. Wullems, with full knowledge of his actions, sold the Filmspeler player in his website, enabling users to watch unauthorised content from unlawful sources through a pre-installed add-ons, and that by doing so, Filmspeler offered its users direct access to unauthorised content, and that this must consequently be regarded as communication to the public within the meaning of Article 3 (1).⁸⁷ The CJEU also noted that Mr. Wullems did not operate under *bona fide* terms, as he himself had marketed Filmspeler as allowing users to watch unauthorised content.⁸⁸ In addition to this *intent* dimension highlighted as pivotal by the CJEU, the court also recognised that the sale of Filmspeler was motivated by profit making.⁸⁹ In light of all this, the CJEU ruled that the conduct of Mr. Wullems amounted to communication to the public. Importantly to us, the CJEU provided that:

*‘It must also be held that, as a rule, temporary acts of reproduction, on a multimedia player such as that at issue in the main proceedings, of copyright-protected works obtained from streaming websites belonging to third parties offering those works without the consent of the copyright holders are such as to adversely affect the normal exploitation of those works and causes unreasonable prejudice to the legitimate interests of the right holder ...’*⁹⁰

The court essentially affirmed that not only those who *provide* and *operate* unlawful streaming services can be considered liable for copyright infringement, but also those who *access* and *use* such services. Filmspeler broadens the framework for liability in copyright infringement cases, and this is certainly something that rights holders will look to make use of. Following the case, it seems that unlawful streaming is now comparable to that of unlawfully downloading material, and this is definitely a victory for EU rights holders, as they are now in a position from where they have more grounds to combat unlawful streaming websites, and use *Filmspeler* as precedent in doing so. In particular, the author believes that the implications of *Filmspeler* will take the form of a rise in the amount of enforcement measures, such as injunctions, against ISPs, compelling them to block access to streaming websites which facilitate piracy. Regarding the Netherlands and the aftermath

⁸⁷ Id, at 41 - 42.

⁸⁸ Id, at 18.

⁸⁹ Id, at 51.

⁹⁰ Id, at 70.

of the *Filmspeler* ruling, Stichting Brein reported⁹¹ that only two weeks after the *Filmspeler* ruling, it had been successful in halting 44 sellers from selling ‘set-top’ devices pre-configured for piracy to customers.⁹² Undoubtedly, *Filmspeler* is a major win for those advocating stronger copyright enforcement mandates in the EU, as streaming unauthorised content has been affirmed to be able to give rise to liability under EU law, and rights holders are consequently better positioned to combat streaming services which facilitate piracy.⁹³

5.1.5 *The Pirate Bay*: primary liability and torrent websites

On the 14 June 2017, the CJEU issued its long awaited ruling in *The Pirate Bay (TPB)* case.⁹⁴ The case concerned two Dutch ISPs (Ziggo and XS4LL), as well as the Dutch copyright foundation Stichting Brein. At the national level, Stichting Brein had requested an injunction ordering the two ISPs to block access to several domain names and IP addresses directing end-users to TPB websites, contending that the website was used by a significant number of the ISPs customers to share copyright protected content, and that it wanted to prevent the ISPs services from being used by consumers to partake in such copyright infringing activities.⁹⁵ Following Stichting Brein’s failed attempts to receive the order against the ISPs in the lower instances, it appealed the matter to the Supreme Court of the Netherlands, who then referred questions to the CJEU, essentially asking whether an intermediary website, like TPB, is communicating to the public works within the meaning of Article 3 (1) of the EUISD. After a 20-month-long wait, the CJEU has now finally handed down its judgement, where it upholds the conclusion reached by *AG Szpunar*,⁹⁶ ruling that making available and managing an online sharing platform, such as TPB, must be considered an act

⁹¹ News provided in the official website of Stichting Brein. <https://stichtingbrein.nl/nieuws.php?id=456> (accessed 20.6.2017).

⁹² TorrentFreak, BREIN ‘Hunts Down’ Pirate Media Player Vendors. May 12, 2017. <https://torrentfreak.com/brein-hunts-down-pirate-media-player-vendors-170512/> (accessed 20.6.2017).

⁹³ Eleonora Rosati, ‘*Filmspeler*, the right of communication to the public, and unlawful streams: a landmark decision’, 27 April 2017. <https://ipkitten.blogspot.fi/2017/04/filmspeler-right-of-communication-to.html> (accessed: 21.5.2017).

⁹⁴ Case C-610/15, *Stichting Brein v Ziggo BV, XS4ALL Internet BV*, Judgement of the Court (Second Chamber), 14 June 2017, ECLI:EU:C:2017:456.

⁹⁵ *Id.*, at 9. As has been previously discussed, TPB functions as an intermediary website in BitTorrent file-sharing schemes, where it indexes *torrents* so that users may locate content from other users computers.

⁹⁶ Opinion of Advocate General Szpunar, Case C-610/15, *Stichting Brein v Ziggo BV, XS4ALL Internet BV*, 8 February 2017, ECLI:EU:C:2017:99, at 85.

of communication under Article 3 (1) of the EUISD.⁹⁷ Following the ruling, it would seem that the extent of a websites good/bad faith goes a long way to determine whether the website can be considered liable for copyright infringement or not. Naturally, more potent measures under Article 8 (3) of the EUISD can be taken where a websites liability is judicially confirmed, and for this reason, we will now move on to highlight the criteria used by the CJEU to determine what kind of websites may be considered breaching copyright holders communication to the public right.

The CJEU started its analysis by stating that, according to settled case law, ‘communication to the public’ should be interpreted broadly, as Article 3 (1) of the EUISD does not define the scope of the concept, and the provision should therefore be interpreted in line with the objective of the Directive, which is to ensure a high level of protection to rights holders, and to make sure that rights holders are able to obtain remuneration for their protected works.⁹⁸ In examining whether TPB communicated to the public unauthorised content, the CJEU provided that, on a preliminary note, it is necessary to examine first whether there is an *act of communication*, and second, whether there is a *public* involved.⁹⁹ The Court highlighted that an act of communication in this context is made when a user *knowingly intervenes to provide access to a protected work*, which can be measured in terms of how fundamentally a website contributes to piracy.¹⁰⁰ The marketing of the website together with its interface and design may further show the *intent* of the website operator, and in the case of TPB, the court noted that the website provided a search engine, as well as systematically structured and categorised torrents in a way that end-users could easily locate unauthorised copyright protected works. Regarding the concept ‘public’, the Court restated that, according to settled case law, it refers to an *indeterminate* and large number of potential viewers, and that it also entailed that the public receiving the communication was ‘new’ in the sense that they had not been taken account of when the copyright holders initially communicated the works to the public.¹⁰¹ Following this, the CJEU concluded that any act made with full knowledge of its consequences and with a view to provide clients with access to protected works is to be considered an act of

⁹⁷ Case C-610/15, *Stichting Brein v Ziggo BV, XS4ALL Internet BV*, Judgement of the Court (Second Chamber), 14 June 2017, ECLI:EU:C:2017:456, at 39.

⁹⁸ *Id.*, at 21 - 22.

⁹⁹ *Id.*, at 24 - 25.

¹⁰⁰ *Id.*, at 26.

¹⁰¹ *Id.*, at 27 - 28.

communication within the meaning of Article 3 (1) of the EUISD.¹⁰² The Court reached this conclusion by examining, first, whether TPB *communicated* works, and secondly, whether there was a *public* to whom the communication was directed at. The following case-specific considerations were highlighted as contributing to the finding that TPBs functioning amounted to communication of works:

- (1) the fact that TPB made it possible for end-users to obtain and share works wherever and whenever they wanted to do so;
- (2) the fact that, although TPB operators did not themselves upload torrents of protected works, they nevertheless managed and made the website available to users, thus knowingly intervening with a view to make the sharing of unauthorised files easier;
- (3) the fact that TPB plays an essential role in making works available to end-users; and,
- (4) the fact that the design of TPB revealed that it intends to index torrents in a way which makes it easy for end-users to locate and download protected content through their services, and that it further deleted faulty torrents and actively filtered some content, with a view to keep the platform as user-friendly as possible.¹⁰³

After affirming that making available and managing an online sharing platform such as TPB must be considered satisfying the communication aspect of Article 3 (1) of the EUISD, the CJEU went on to examine whether such communication satisfied the second requirement also, *i.e.* the 'public' aspect of Article 3 (1). The Court noted that the *de minimis* principle, which excludes small and insignificant groups of persons from qualifying as a public, could not be relied on by TPB, as it was apparent from the order for reference submitted by the Supreme Court of the Netherlands that a significant number of the ISPs customers had indeed downloaded files through TPB, and furthermore, TPB had itself bragged that its services were being used by millions of users. Because the functioning and operation of TPB was aimed at an indeterminate number of end-users, the Court provided that it consequently satisfied the 'public' requirement in Article 3 (1).¹⁰⁴

¹⁰² *Id.*, at 34.

¹⁰³ *Id.*, at 35 - 38.

¹⁰⁴ *Id.*, at 42 - 43.

Having affirmed that TPB must be considered unlawfully communicating works under Article 3 (1) of the EUISD, the CJEU went on to highlight that (1) TPB operators were *well aware* of the fact that their website was used to share unauthorised content, (2) that they made *economic profit* in operating the website, and (3) that TPB operators expressly made it clear in blogs and forums accessible through the site that they *encouraged* end-users to share copies of copyright protected content using their service. Following these findings, the CJEU concluded that making available and managing a sharing online platform such as TPB, which indexed metadata allowing users to locate and download protected works using P2P networks, constituted communication to the public within the meaning of Article 3 (1).¹⁰⁵ The case essentially affirms that, provided that a website plays an essential role in making protected works available, it may be held primarily liable for copyright infringement, despite the fact that unauthorised content is placed to the website by end-users and not the website itself. The liability of a website becomes all the more apparent if the website operates with the intention of making financial gain in doing so, which was the case with TPB, who had been shown to receive substantial advertising revenues from operating the TPB.

5.2 Interim conclusions

We addressed the relevant CJEU preliminary rulings and highlighted the constraints that need to be kept in mind when looking to make use of Article 8 (3) of the EUISD as against ISPs. Since the use of injunctions against ISPs in file-sharing cases is becoming increasingly more ordinary among rights holders looking to implement their copyright enforcement strategy, ISPs are transforming more and more into copyright enforcers in the online environment, something that many people are worried about. The author of this thesis, although acknowledges the dangers associated with transforming ISPs into ‘internet copyright police’, still believes that it is necessary to involve ISPs in the fight against piracy if rights holders are to be able to adequately protect their IPRs in the online environment. Especially with respect to injunctions, the author is not too worried about the new obligations (and powers) of ISPs, as injunctions are generally court issued orders, and thus a degree of judicial oversight remains in place to make sure that enforcement of IPRs remains in balance with other considerations relevant in the file-sharing context, like the privacy of end-users and website operators right to freedom of expression. So long as there is judicial oversight over the

¹⁰⁵ Id, at 45 - 48.

granting of injunctions, the author is content that enforcement initiatives will be subject to adequate checks and balances by the courts. It has become clear that copyright holders must always look to implement a balanced enforcement strategy, and respect the principle of proportionality in doing so. Further, they must strike a balance between conflicting fundamental rights, seek measures which are effective and suitable for the purposes combating infringements of their rights, and they may not require ISPs to conduct general monitoring of their services.

We will move on to examine interesting instances of domestic application of Article 8 (3) of the EUIPD, as well as highlight other national ‘innovations’ constituting best practices in the context of combating piracy and involving ISPs in the fight against such piracy.

6. Best practices and latest developments at the EU Member State level

6.1 Domestic application of Article 8 (3) of Directive 2001/29/EC against internet service providers

Member States of the EU have been left to transpose and implement the various EU directives under their own discretion, and they have taken different approaches in doing so. With regard to Article 8 (3) of the EUISD, some countries have transposed Article 8 (3) without modification of its original version, more or less verbatim to the original provision as provided for in the Directive, whereas other countries have enacted detailed regulation implementing the said Directive.¹⁰⁶ Member States may go further beyond what the directive explicitly requires and provide for more stringent protection and enforcement measures, so long as these are provided with a view to ensure a high level of protection to rights holders, and remain in conformity with EU law, CJEU case law constraints, and strike a fair balance between competing fundamental rights interests. We will now highlight domestic initiatives amounting to best practices in the piracy/ISP context.

6.1.1 Sweden: *Swefilmer* as a landmark case

Under the Swedish copyright legal framework, injunctions can be issued on the basis of Section 53b of the Swedish Copyright Act, which provides that a court may prohibit a party from contributing to or committing copyright infringement.¹⁰⁷ Essentially, this is the Swedish law implementing Article 8 (3) of the EUISD. Section 53b of the Swedish Copyright Act provides that injunctions under copyright law may be issued when the addressee has been found primarily or secondarily liable for copyright infringement. Further, according to the legislators preparatory materials, operating a network does not *per se* constitute facilitation of copyright infringement, and consequently, it has been hard for rights holders to obtain such injunctions against ISPs in Sweden. Due to this reason, for a long time, not a single ISP was compelled to implement blocking measures at the user-end. However, on the 28th February 2017, this all changed when the Swedish Court of Patent Appeals and the Market Court,¹⁰⁸ drawing upon CJEU constraints as provided for in *UPC Telekabel Wien*, ordered the defendant ISP *Bredbandsbolaget* (B2) to block access to URLs directing to the torrent

¹⁰⁶ Pekka Savola, “Proportionality of Website Blocking: Internet Connectivity Providers as Copyright Enforcers,” 5 JIPITEC 116, at 25 [2014].

¹⁰⁷ Article 53b of the Swedish Act on Copyright in Literary and Artistic Works (1960:729).

¹⁰⁸ *Patent- och Marknadsdomstolen*; a Swedish appeals court with exclusive jurisdiction in IPR litigation.

indexing website *TPB*, as well as the popular Swedish streaming portal *Swefilmer*.¹⁰⁹ In the first instance, the Stockholm District Court ruled that the conduct of B2 (providing internet access to consumer who partook in piracy) did not amount to participation in a crime under Swedish law, and consequently, it refrained from granting the plaintiffs the blocking order they sought. The plaintiffs (including Universal Music, Sony Music Entertainment, Warner Music, and Nordisk Film) appealed the decision, and argued that the EUIRD required Member States to make sure that injunctive relief may be sought as against intermediaries whose services are being used by third parties to commit infringements, and that by empowering its customers with internet connection, B2 was objectively abetting the infringement of their copyright protected musical and film works, and should be considered an intermediary within the meaning of Article 8 (3) of the EUIRD. B2, on the other hand, argued that its purely technical function could not be considered involvement in breach of copyright law.

The Swedish Court of Patent Appeals and the Market Court considered CJEU court practice, and concluded that its case-law clearly provided that an order may be issued against an intermediary, such as an ISP, for simply providing internet connection that is utilised in copyright infringing activities, even though the ISP could not be considered colluding with its customers in the criminal sense. It stated that there is no need for B2 to be criminally liable for copyright infringement in order for it to be subject to an injunction, and that the national law provision requiring so should be interpreted in conformity with EU law (the *Marleasing* principle). After the CJEU was content that B2 qualified as an intermediary within the meaning of Article 8 (3) of the EUIRD, it moved on to conclude that there is no possibility of using less restrictive measures to effectively enforce copyright in the case. The court provided that the Swedish Copyright Act should be interpreted in light of EU law, and following this, the Appeals Court overturned the earlier ruling issued by the District Court, and ordered B2 to implement a 3-year block towards the identified infringing websites,¹¹⁰ subject to a fine of SEK 500,000 — the equivalent of roughly 53,000 EUR — in case

¹⁰⁹ Swedish Court of Patent Appeals and the Market Court, case 11706-15 (2017). The blocking order contained 5 web addresses in relation to *Swefilmer*, and 323 addresses in relation to *The Pirate Bay*. *Swefilmer* has been said to serve up to 25% of all online video streaming activities in Sweden. See: *TorrentFreak*, "*Streaming Site Operator Jailed For Three Years After Landmark Trial*". May 16. 2017. <https://torrentfreak.com/streaming-site-operator-jailed-for-three-years-after-landmark-trial-170516/> (accessed 22.6.2017).

¹¹⁰ The identified domain names and URLs are listed in Appendix 3 of the ruling.

of non-implementation.¹¹¹ The Patent and Market Court of Appeal decided not to allow an appeal of its judgement to the Swedish Supreme Court, and the ruling would appear to be final as such.¹¹²

The *Swefilmer* ruling is a landmark victory in Sweden, as it paves the way for blocking injunctions against ISPs in the file-sharing context. Although the injunction against B2 concerned a limited amount of websites, the case opens the door to wider injunction mandates which may potentially contain hundreds of identified infringing URLs, or even more. Most importantly, however, the case has made it official that website blocking can be successfully implemented in Sweden, and this enhancement in the level of protection afforded to copyright holders in Sweden owes itself to EU copyright law, and in particular, that of Article 8 (3) of the EUIPD.

The Court of Appeals Judge, *Christine Lager*, stated right after handing down the ruling that:

*“In today’s judgment, the Patent and Market Court held that right holders such as film and music companies can obtain a court order in Sweden against a ISP, which forces the ISP to take measures to prevent copyright infringement committed by others on the internet. The decision is based in EU law and Swedish law should be interpreted in light of EU law. Similar injunctions have already been announced, such as in Denmark, Finland, France and the UK, but the verdict today is the first of its kind in Sweden.”*¹¹³

The ruling is undoubtedly good news for Swedish rights holders, as the real possibility of utilising Article 8 (3) of the EUIPD has only now following the *Swefilmer* ruling been explicitly made possible under Swedish law, and this has been welcomed by the Swedish Film Industry, as becomes apparent from the comment made by the entertainment industry spokesperson Per Strömbäck:

*“It is good that the legal situation has now been made clearer. We know from Denmark, Norway and Finland that these measures are effective and legally sound.”*¹¹⁴

¹¹¹ Swedish Court of Patent Appeals and the Market Court, case 11706-15, at 30 (2017).

¹¹² *Id.*, at 34.

¹¹³ TorrentFreak, “The Pirate Bay Must Be Blocked in Sweden, Court of Appeal Rules”. February 13, 2017: <https://torrentfreak.com/the-pirate-bay-must-be-blocked-in-sweden-court-of-appeal-rules-170213/> (accessed 20.6.2017).

¹¹⁴ The Local, 13 February 2017: “Swedish broadband provider must block The Pirate Bay, court rules,” <https://www.thelocal.se/20170213/swedish-broadband-provider-must-block-the-pirate-bay-court-rules> (accessed: 20.6.2017).

The *Swefilmer* case is a perfect example of the importance of EU copyright law in affording copyright holders a high level of IPR protection in the EU. Swedish law itself was not apt to enable rights holders make ISPs implement website blocks at the user end, but now, following *Swefilmer* and the pro-EU interpretation given to Article 53b of the Swedish Copyright Act, rights holders are better placed to combat unlawful file-sharing, and may compel ISPs to collaborate in mitigating infringing activities conducted by their customers. This can further be done against P2P file-sharing websites, like torrent indexing websites, as well as streaming websites, which make available content without rights holders consent.

Now that the first ISP in Sweden has been ordered to implement website blocking at the user-end, the next matter which will surely become topical is whether other ISPs will move on to implement the same measures that B2 needs to implement. Per Strömbäck, representing the TV and film industry sectors in Sweden, has stated that:

*“We believe that the legal situation is now clear and that ISPs should act in unison with B2 Bredband and apply the same measures [to block The Pirate Bay and Swefilmer]. We hope that we will now get to the same position as in Norway, Denmark and the UK, where telecom operators cooperate on blocking pirate websites”.*¹¹⁵

Essentially, the statements go on to show that the entertainment industry wants all the ISPs to collaborate and act accordingly to the *Swefilmer* ruling. To the author of this study, it seems logical that other ISPs are required to implement similar measures as those that B2 has been ordered to implement, unless a given ISPs cannot be considered to have any infringing customers, something which will be very hard for an ISP to show true. Nevertheless, it is likely that other ISPs will resist enforcement obligations for as long as they can, and only implement such measures when they are explicitly required to do so by a court of law. Thus, further litigation on the matter is like to emerge, unless ISPs move on to *voluntarily* implement enforcement measures following obligations other ISPs have been subject to. In the authors opinion, resistance, rather than voluntary implementation, will occur. ISPs will make arguments that blocking measures can be easily bypassed, using for

¹¹⁵ C. Cooke, ‘Major Swedish ISP says it won’t web-block without a court order,’ 22 February, (2017). <http://www.completemusicupdate.com/article/major-swedish-isp-says-it-wont-web-block-without-a-court-order/> (accessed 20.6.2017).

example VPNs or proxies, and are thus ineffective for the purposes of protecting IPRs, or that it is unfair that they need to assume implementation costs for protecting rights holders copyright. For example, following the ruling in *Swefilmer*, the ISP *Telia*¹¹⁶ has stated that it is not going to block *TPB* in Sweden until it is ordered to do so by the judiciary.¹¹⁷ This is problematic in many regards, and it is undoubtedly very much unfair that *one* ISP is required to implement measures which another similar ISP is not required to do. These issues will surely become the subject of further litigation in the near future, but it is like to take some time before more clarity on the matter is reached. On the positive side, such resistance will lead to new considerations provided by courts, and checks and balances will be conducted again. It is by no means stipulated that protection of IPRs is absolute, as has been confirmed in *UPC Telekabel Wien*,¹¹⁸ and it is important to protect ISPs fundamental rights also, and make sure that there is a constant balancing of rights going on between rights holders, ISPs, and any other affected parties. When one fundamental right is afforded more protection than another, this must always be justified, and justification can only be done following adequate balancing of rights. It is submitted here that such balancing tests need to be conducted before requesting for injunctive relief from the courts.

The *Swefilmer* case is a significant ruling in paving the way for website blocking in Sweden, and will surely in the near future act as precedent for copyright holders to argue that more stringent and extensive blocking should be implemented by ISPs, as well as that such enforcement measures should be implemented by other ISPs also in addition to B2, who was explicitly considered in the *Swefilmer* ruling. Regarding whether other Swedish ISPs will voluntarily move on to implement similar measures as their competitor counterparts have been ordered to do, this is a problem which will likely be solved by the Swedish courts. It could be greatly beneficial for Swedish ISPs to follow the example set by their neighbouring country, Denmark, where ISPs have come up with a simple, yet extremely significant solution for this problem, which levels the playing field for Danish ISPs, and simultaneously, makes them collectively stronger. Collaboration among ISPs is notably

¹¹⁶ A notable ISP in the Nordic European region.

¹¹⁷ C. Cooke, ‘Major Swedish ISP says it won’t web-block without a court order,’ 22 February, (2017). <http://www.completemusicupdate.com/article/major-swedish-isp-says-it-wont-web-block-without-a-court-order/> (accessed 20.6.2017).

¹¹⁸ Judgment of 27 March 2014, *UPC Telekabel Wien* (C-314/12), EU:C:2014:192, at 61 - 63.

strong in Denmark, and we will move on to examine how such collaboration serves to benefit not only Danish ISPs, but Danish rights holders also.

6.1.2 Denmark: Code of Conducts and one-stop-shop blocking

Denmark has been one of the EU Member States which has taken a leading role in combating piracy within its jurisdiction. In 2006, the Danish Supreme Court gave the first blocking injunction order in the EU ordering the Russian *AllOfMP3* website to be blocked,¹¹⁹ and in 2010, in the so-called *Danish TPB* case, the Danish Supreme Court became the first Supreme Court in the EU to grant a user-end blocking order based on Article 8 (3) of the EUISD.¹²⁰ Today in 2017, there is strong precedent in Denmark allowing for ISPs to be subject to injunctions in piracy cases, and it may be said that the Danish copyright enforcement framework is among the most stringent ones in the EU.

In respect of the problem that has now become topical in Sweden following the ruling in *Swefilmer*, Denmark provides for a solution on the matter. In September 2014, the Danish Telecom Industry Association (*Teleindustrien*), signed a voluntary Code of Conduct (CoC)¹²¹ with local ISPs, whereby they agreed to implement a blocking injunction within seven days notification after a particular ISP has been ordered by a court to do so.¹²² Essentially, and in the words of *Maria Fredenslund*, the CEO of the Danish Rights Alliance,¹²³ the CoC aims at “*setting up a one stop shop for website blockings at DNS level.*”¹²⁴ This greatly streamlines online copyright enforcement procedure in Denmark, as a single ruling issued against a single ISP creates a ripple effect, which requires all other ISPs to implement similar mandates contained in the injunction originally directed towards only a certain ISP.

¹¹⁹ IFPI Denmark v Tele2 A/S, Case F1-15124/2006, 25 October 2006 (City Court of Copenhagen).

¹²⁰ Sonofon A/S v. IFPI Denmark, Case 153/2009, 27 May 2010 (Supreme Court of Denmark).

¹²¹ The CoC, in Danish language, can be accessed here: <http://www.teleindu.dk/wp-content/uploads/2014/10/TI-code-of-conduct-blokeringer.pdf> (accessed 22.5.2017).

¹²² Maria Fredenslund, “Denmark: Code of Conduct on website blocking,” *RettighedsAlliancen*, (2014). Available here: <http://kluwercopyrightblog.com/2014/10/24/denmark-code-of-conduct-on-website-blocking/> (accessed 20.6.2017).

¹²³ See: <http://rettighedsalliancen.dk/om-os/> (accessed 20.6.2017). The Danish Rights Alliance represents more than 100,000 Danish rights holders.

¹²⁴ Maria Fredenslund, “Denmark: Code of Conduct on website blocking,” *RettighedsAlliancen*, (2014). Available here: <http://kluwercopyrightblog.com/2014/10/24/denmark-code-of-conduct-on-website-blocking/> (accessed 20.6.2017).

The CoC is a voluntary agreement, and it does not preclude its members from reserving the right to have their case reviewed separately, if this is indeed appropriate due to objectively justifiable reasons. The use of voluntary CoCs is encouraged in the IP Enforcement Directive, which provides in its Article 17 that associations and organisation based in Member States are encouraged to use such CoCs aimed at contributing towards enforcement of IPRs. Article 16 of the eCommerce Directive also provides that Member States are encouraged to use CoCs with a view to contribute to the proper implementation of the Directive. Rights holders in Denmark may take strategic steps to apply for an injunction against the most attractive ISP (litigation-wise), without having to take action against all ISPs separately, like would seem to be the case currently in Sweden; ISPs, on the other hand, are placed on a fairer and more advantageous footing, as there will be no situation where one ISP assumes burdens which another ISP does not, like is the case with B2 in Sweden, and further, if ISPs feel they are disproportionately affected by a given order, they may jointly challenge the injunction. If the goal is to arrive to a mutually beneficial relationship, rights holders and ISPs should not view one-another as enemies, but rather, as partners, who can benefit from one another, and who can tackle new challenges in collaboration, with a view to do so swiftly and without having to engage in years of expensive litigation. In this regard, Danish ISPs definitely set a model example for other ISPs around the EU, and the author of this study highlights the Danish case of voluntary collaboration among ISPs as an instance of *best practice*, something other Member States of the EU are advised to take note of.

6.1.3 United Kingdom: live blocking orders as the forthcoming trend in the European copyright enforcement arena?

Although the UK is in the process of leaving the EU, it is nevertheless beneficial for us to consider the UK perspective to combating unlawful file-sharing, as the UK courts have issued insightful rulings on intermediary liability, and they have done so in light of EU law. In the UK, the national provision implementing Article 8 (3) of the EUIPD is Section 97A of the Copyright, Designs and Patents Act 1988 (CDPA), which essentially provides that the High Court may issue injunctions against service providers who have "*actual knowledge of another person using their service to infringe copyright*". Due to the plentiful amount of cases regarding the application of Section 97A

of the CDPA, there is a relatively solid basis for blocking injunctions in the UK.¹²⁵ The first blocking injunction against an ISP was granted in 2011 in the so-called *Newzbin2* case,¹²⁶ and more blocks against copyright infringing websites have been implemented by ISPs since then.¹²⁷ Website blocking has been part of UK rights holders enforcement strategy for quite some time now, and using injunctions to combat infringements has also become trendy in other fields of IPR law.¹²⁸ The UK IPR enforcement framework is among the most stringent ones in the EU, possibly owing to the fact that the IPR industry is exceptionally big in the UK, as well as the fact that a very substantial amount of IPR-related infringements occur in the UK.¹²⁹

We will consider an extremely interesting landmark decision handed down by the England and Wales High Court on the 13th of March 2017, in *Football Association Premier League v British Telecommunications* (*'Premier League'*), where the first *live* blocking order under Section 97A of the CDPA was granted against six main ISPs in the UK,¹³⁰ compelling them to block access to *streaming servers* through which unauthorised copyright protected content was being made accessible.¹³¹ No such live blocking has been ordered before in the UK (or any other EU country according to the author's knowledge), and the ruling is significant in paving the way for more potent and creative enforcement strategies that rights holders may pursue with a view to protect their copyright through ISPs. Although the ruling regards copyright law in the UK, rights holders in other EU countries may also take steps to pursue a similar case as *Premier League*, with a view to set precedent in their own respective countries. This can best be done after carefully analysing *Premier League*, especially with respect to the proportionality considerations contained in the

¹²⁵ As noted by Justice Arnold in *Football Association Premier League Ltd v British Telecommunications Plc & Ors* [2017] EWHC 480 (Ch) (13 March 2017), at 5.

¹²⁶ *Twentieth Century Fox Film Corp & Ors v British Telecommunications Plc* [2011] EWHC 1981 (Ch).

¹²⁷ For example in *Football Association Premier League Ltd v British Sky Broadcasting Ltd & Ors* [2013] EWHC 2058 (Ch).

¹²⁸ For example, with respect to trademark enforcement, see *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors* [2014] EWHC 3354 (Ch).

¹²⁹ For example, it has been stated that 7.2 billion visits to copyright infringing streaming websites took place in the UK in 2016, which is a 60% increase compared to the figure in 2015. *See*: TorrentFreak, "Hold ISPs Responsible for Piracy After Brexit, Music Biz Says". May 12, 2017. <https://torrentfreak.com/hold-isps-responsible-for-piracy-after-brexit-music-biz-says-170512/> (accessed 22.6.2017).

¹³⁰ More specifically, British Telecommunications, EE, Plusnet, Sky, TalkTalk, and Virgin.

¹³¹ *The Football Association Premier League Ltd v British Telecommunications Plc & Ors* [2017] EWHC 480 (Ch).

ruling, as the case essentially serves to show that ISPs may be compelled to implement very potent measures, as long as such measures satisfy proportionality requirements.

The Football Association Premier League (FAPL) witnessed a growing problem of its content (live Premier League sports footage) being made available online through streaming portals without its due authorisation. It submitted as much to the court, and the judge (Justice Arnold) accepted this, noting that consumers increasingly more often use interfaces such as apps and media players to view unlawful streams and content, instead of doing so via traditional web browsing.¹³² In the case, FAPL was granted an injunction compelling six main retail ISPs to implement blocking measures towards identified ‘target streaming servers’, which facilitated copyright infringements by broadcasting Premier League footage without the rights holders due authorisation. The order granted is unprecedented and innovative in various ways: first off, it is a live blocking order, as it is to be implemented only when Premier league games are being broadcast live.¹³³ Secondly, the order requires that the listed target servers are *re-set* each week when the Premier League season is on, thus ensuring that blocking remains targeted towards infringing activities.¹³⁴ Thirdly, time-wise, the order is of a very limited nature, as it is to be effective only from 18 March 2017 to the 22 May 2017, *i.e.* when the Premier League season is on.¹³⁵ This further highlights the proportionality of the order, as the rights holders have identified the time within which infringements are envisaged to occur, instead of requiring ISPs to implement such measures for an unlimited period of time. Fourthly, the order stipulates that each hosting provider must be informed in advance (by notice) when blocking is to be implemented, thus affording time for the addressee of the block to challenge the it when appropriate.¹³⁶ Justice Arnold considered it clear that the defendants internet services were pivotal for UK users to be able to access the target servers, and after accepting that the ISPs networks incurred significant traffic spikes when Premier League footage was being broadcasted, and that the ISPs had actual knowledge of their services being used to infringe copyright (as they

¹³² Id, at 10 - 11.

¹³³ Id, at 24.

¹³⁴ Id, at 25.

¹³⁵ Id, at 26.

¹³⁶ Id, at 27.

had been informed as much by copyright holders monitoring the infringing activities), the judge ultimately went on to grant the injunction against the defendants as sought by FAPL.¹³⁷

However, before granting the injunction, the court considered the following important aspects of the order sought, with a view to ensure that the order sought was *proportionate* and suitable for the purposes of protecting copyright: whether the order sought by FAPL was *effective and dissuasive* for its purposes, whether there existed *alternative measures* that could have been better fit for the rights holders purposes, whether the order sought was *unnecessarily complicated or costly*, whether the order constituted *a barrier to trade*, and finally, whether *adequate safeguards* were in place to protect the various parties fundamental rights.¹³⁸ These considerations are of utmost importance when determining whether to grant or to refuse granting injunctive relief to copyright holders, as the considerations ultimately serve to help courts and rights holders alike conclude whether a given order sought or copyright enforcement strategy satisfies the important *principle of proportionality*, which has been recurrently deemed pivotal in piracy and intermediary liability cases.

First, the court considered whether the order sought by FAPL was *effective and dissuasive*. Justice Arnold referred to a study published by Carnegie Mellon University supporting the conclusion that blocking measures implemented by ISPs have been shown to reduce the number of UK users who engage in copyright infringing activities via websites (according to the study, a 22% overall reduction in piracy was observed for users affected by blocks), and as a consequence, the legal consumption of content via lawful interfaces had increased following such blocking (according to the study, Netflix incurred a 6% increase in consumption of its services).¹³⁹ Justice Arnold noted that blocking access to streaming servers would be more effective than implementing measures against individual websites making available such links directing to streams, and this further affirmed his opinion that the order sought was in fact effective and dissuasive. Finally, after accepting that the monitoring and blocking techniques employed by both FAPL and the defendants had improved from the measures implemented before due to advances in technology, thus allowing for the mitigation of a greater proportion of potential infringements, and following the finding that

¹³⁷ Id, at 70.

¹³⁸ Id: paragraphs 48 - 54 (*effectiveness and dissuasiveness*); paragraphs 57 - 63 (*alternative measures*); and, paragraph 64 (*unnecessarily complicated or costly*).

¹³⁹ Id, at 49 - 50.

blocking the target streaming servers could have an educative effect on the public in the UK (raising awareness regarding the illegality of streaming unauthorised content), Justice Arnold concluded that the order sought was, in his opinion, effective and dissuasive, and moved on to consider whether alternative measures more apt to the infringements existed.¹⁴⁰

FAPL argued that the other means available to combat the infringements of its rights via streaming were ineffective or incomplete to adequately combat the problem. The court pinpointed several issues which supported the argument put forward by FAPL. First, regarding the practice of sending *takedown notices* to streaming server operators, the court noted that although FAPL and its licensees had taken real *bona fide* steps to contact server operators and ask them to stop allowing for streaming of unauthorised content, only some complied with the requests, while many did not.¹⁴¹ This goes a long way to show how takedown notices are only effective when dealing with *bona fide* servers providers, something not like to be the case with streaming server operators who knowingly facilitate piracy and make available or communicate copyright protected content online. The court also acknowledged that pursuing direct action against hosting providers who hosted such streaming websites was impracticable or impossible because almost all hosting providers used by streaming server operators were based overseas and registered anonymously.¹⁴² This is undoubtedly true, and no wonder besides, as streaming server operators who knowingly facilitate copyright infringements *of course* want to be hosted with offshore service providers, where it is harder to identify them and pursue legal action against them. Further, Justice Arnold noted that the police are generally unwilling to take on and pursue every single copyright prosecution, as there are undoubtedly other more pressing matters which the police need to allocate their time and resources towards. In light of the previous findings, namely, that take down notices have been shown to be inefficient and go largely unregarded, that pursuing action against server operators *directly* is near impossible due to them being anonymous and being hosted offshore, and the fact that the executive authorities lacked motivation, time, and resources to pursue such copyright wrongdoers, Justice Arnold was satisfied that FAPL did not have any other (suitable) alternative measures turn to with a view to protect its copyright.

¹⁴⁰ Id, at 52 - 53.

¹⁴¹ Id, 57 - 58.

¹⁴² Id, at 59.

Regarding the criterion that the order should not be unnecessarily complicated or costly, Justice Arnold held that, owing to the fact that no defendant explicitly challenged the order on grounds of it being unnecessarily complicated or costly, and further, that FAPL and the defendants all positively supported the order with its terms already agreed, with the exception of TalkTalk, which refrained from either endorsing or opposing the order, the judge concluded that there is no order as to costs, and was satisfied that the order was neither unnecessarily complicated nor costly.¹⁴³

Next, the court examined whether the blocks sought by FAPL constituted barriers to legitimate trade. Justice Arnold was of the same opinion with FAPL in that the targeted nature of the order sought *per se* meant that it avoided creating barriers to legitimate trade, and that this was all the more true because the majority of the content being made available by the target servers, if not all of it, was copyright protected content owned by FAPL, or some other rights holder. Justice Arnold noted that, even when the content owned by FAPL was not being streamed, other content made accessible through the streaming portal constituted almost exclusively of copyright protected commercial content, ranging from films and television series to sports broadcasts. It had been shown that some target server operators even blacked out the logo of the channel who owned the domestic rights to broadcast the content, and that this showed how the given streaming server operators engaged in copyright infringing activities knowingly, and thus could not be considered *bona fide* service providers. The court finally reasoned that, although it was possible in theory that a proportion of the content made available by the streaming servers could be lawful, such content is *de minimis* when comparing it to the amounts of infringing content being made available by the streaming servers, and that this ultimately served to outweigh the significance given to the barriers on trade argument.¹⁴⁴

Finally, before moving on to conclude whether the previously discussed aspects of the order could in conjunction satisfy proportionality, the judge very briefly considered whether the order sought had sufficient safeguards in it. It concluded in the affirmative, highlighting the relevance of the especially limited duration of the order, which was to be implemented only when Premier League

¹⁴³ Id, at 62 - 64.

¹⁴⁴ Id, at 65 - 67.

footage was being broadcasted during the season.¹⁴⁵ Here, the judge concluded that it accepted that the order sought by FAPL was proportionate as to its aim, considering the fact that FAPL's rights were being violated at a large scale. The judge deemed the order effective and dissuasive, accepting that it did not constitute a barrier to lawful trade, that no alternative measures apt for the purposes of protecting copyright were available in the case, that the order was not too complicated or costly, and that it contained adequate safeguards.¹⁴⁶

Ultimately, Justice Arnold concluded that he would move on to make the order.¹⁴⁷ This significant ruling has undoubtedly been welcomed by rights holders in the UK, as now that the first live blocking order has successfully been granted, rights holders have greater incentives to combat unlawful streaming portals and require ISPs to block access to them. In requesting for injunctive relief, it is important that rights holders do not lose sight of proportionality; orders must satisfy a great deal of legal requirements, ranging from the measures purported effectiveness to costs of implementing such measures. The nature of orders must be further considered in light of the severity of the copyright violations that have been committed, always taking into consideration whether the subject of the blocking is a *bona fide* service provider, or a bad faith operator knowingly facilitating piracy. The importance of conducting sound proportionality evaluation before pursuing copyright enforcement strategies cannot be stressed enough, as an injunction sought must be proportionate for it to be granted. This is all the more true because ISPs are lawful business entities, who do not act with streaming servers and infringing websites in common design to facilitate copyright infringements, but rather, they are entities whose services are *abused* by such copyright wrongdoers. Because of this, the threshold for issuing injunctions against ISPs should be rather high than low, and orders granted only once it has been accepted that the measure sought satisfies the proportionality requirements.

6.2 Interim conclusions

We have considered three interesting countries and their respective situation with ISP liability and piracy. The trend in the EU seems to be that ISPs are increasingly more often compelled to partake

¹⁴⁵ *Id.*, at 68.

¹⁴⁶ *Id.*, at 69.

¹⁴⁷ *Id.*, at 70.

in copyright enforcement mandates, and the role of EU law in allowing for this to happen has definitely been significant. User-end website blocking is also becoming increasingly more common among EU Member States, with the Danes being the first ones to successfully order website blocking back in 2006, whilst the Swedes have only now in 2017 succeeded in doing so. The principle of proportionality is the single most important notion that rights holders need to consider when looking to implement their copyright enforcement strategies, as proportionality evaluation must be conducted if rights holders want to successfully compel ISPs to collaborate with them in combating piracy online. Article 8 (3) of the EUISD has been significant in raising the level of copyright protection afforded to rights holders in the EU, and it is now clear that Article 8 (3) may be used to compel ISPs to collaborate with rights holders, so long as such mandates are proportionate and strike a balance between competing fundamental rights. Now that the relevant EU law considerations regarding ISPs and injunctions have been considered and domestic best practices have been highlighted, we are in a position to move on to the *analysis* chapter, where we will consider the relevance of proportionality in arriving to a lawful copyright enforcement strategy, highlight proportionality criteria applicable when evaluation the proportionality of website blocking injunctions, and ultimately, set the ground for answering the research question posed in *Section 1.2* of this study.

7. Analysis

7.1 Proportionality as key in determining the legality of injunctions under Article 8 (3) of Directive 2001/29/EC

This section of the study focuses on the proportionality of measures under Article 8 (3) of the EUISD, with special focus on the user-end website block. The Directive itself does not provide for objective guidance on the application of Article 8 (3), and for this reason, the preliminary rulings of the CJEU are of paramount importance to us, as they help us conclude what proportionality *criteria* contribute to formulating a lawful enforcement strategy under Article 8 (3). Although proportionality has been the subject of discussion in CJEU case law concerning Article 8 (3), such discussion has often been given in a rather summary fashion, and it can be hard to extract the specific criteria used in formulating the proportionality evaluation. Nevertheless, we will review and analyse the considerations provided by the CJEU, and further highlight the *criteria* which have been deemed pivotal in the past in determining the legality of enforcement measures under Article 8 (3).

Whereas CJEU case law gives us a general understanding of the nature of proportionality, national cases provide for more specific analysis regarding actual criteria used to evaluate proportionality. This is only logical, as the CJEU does not assume the role of national courts when handing down preliminary rulings, but rather, the CJEU helps national courts with questions regarding the correct *interpretation* of EU law. In user-end website blocking injunctions, proportionality evaluation regards especially the *scope* and *effectiveness* of the measure sought by under Article 8 (3), which needs to be balanced against ISPs freedom to conduct a business, end-users protection of privacy and data, as well as the rights of the website operator, which are often neglected or not adequately represented.¹⁴⁸ Consequently, the importance of proportionality evaluation in granting injunctions cannot be overstated, and therefore, it can be said that proportionality evaluation is *key* in determining the legality of injunctions sought by rights holders under Article 8 (3) of the EUISD.

¹⁴⁸ Website operators have *inter alia* the right conduct a business, freedom of expression, and the right to a fair trial.

7.1.1 Internet service providers as mere conduit intermediaries

On a preliminary note, we should remind ourselves that, in the EU, ISPs are generally exempted from being held liable for their customers infringing activities, provided that certain conditions are satisfied.¹⁴⁹ The lack of direct liability attributed to ISPs is based on their technical functioning, which is neutral and passive. Under the eCommerce Directive, this implies lack of knowledge and control over the data transmitted, *i.e.* the lack of knowledge of their customers activities.¹⁵⁰ To balance this situation, courts may issue injunctions against ISPs, compelling them to address infringements of copyright occurring through their services.¹⁵¹ Because ISPs do not control the activities of their customers, but merely provide for internet connectivity services, injunctions *must* be proportionate, and cannot entail excessive liability upon ISPs, as they have the right to conduct a business, and applying broad and disproportionate measures against them would give rise to various fundamental rights concerns, as well as stifle innovation and amount to preventive censorship.¹⁵²

7.1.2 The importance of balancing competing interests

Proportionality evaluation entails considerations regarding both the *private* interests of the parties to the proceedings, as well as *public* interests relevant to society as a whole. Whereas private considerations relate to matters such as protection of IPRs and the right to conduct a business, public considerations relate to innovation policy, market economy, network neutrality, and ultimately, democracy and freedom of expression. All of this must be taken into consideration when evaluating proportionality of blocking injunctions, because, as has been affirmed in *UPC Telekabel Wien*, the protection of IPRs is *not* absolute, and must be balanced against other competing interests.¹⁵³ Ideally, rights holders should conduct such proportionality balancing tests before applying for injunctions, as else they risk being denied injunctive relief on grounds of disproportionality. A proportionate injunction-request may be achieved by carefully examining the trade-offs of the request, such as the costs and burdens of implementation, effectiveness of measure,

¹⁴⁹ Namely, Articles 12 - 14 of the eCommerce Directive.

¹⁵⁰ Recitals 42 - 44 of the eCommerce Directive.

¹⁵¹ In the EU, this possibility is secured by Article 8 (3) of the EUIDS.

¹⁵² J. Blevins, "Uncertainty as Enforcement Mechanism: The New Expansion of Secondary Copyright Liability to Internet Platforms", 34 *Cardozo Law Review*, at 1825 [2013].

¹⁵³ Judgment of 27 March 2014, *UPC Telekabel Wien* (C-314/12), EU:C:2014:192, at 61.

restrictions on parties, and other impacts following the possible grant of the injunction. What constitutes proportionality may be specified at the national level, but such considerations can hardly be codified exhaustively. Ultimately, it falls to the relevant authorities to address injunctive relief requests and determine whether they satisfy proportionality requirements.

7.1.3 Lessons learned from *Scarlet Extended*: Article 15 (1) of the eCommerce Directive and blanket monitoring

The *Scarlet Extended* ruling discussed previously in this study provides us with food for thought regarding proportionality of measures under Article 8 (3) of the EUIPD. The enforcement measure sought in the case was a filter, which was to be implemented by the ISP (Scarlet) against its customers, with a view to keep its services from being used to access copyright infringing websites on a preventive note. The filter in question was of a particularly wide nature, as it was to apply indiscriminately to *all* of Scarlets users and communications, for an *indefinite* period of time, and *solely* at the expense of the said ISP. The filter also gave rise to over-blocking, as it could not adequately enough distinguish between infringing and lawful content. Ultimately, the CJEU deemed the measure disproportionate and unlawful, as its implementation would have required Scarlet to conduct *de facto* general monitoring of its network, something prohibited by Article 15 (1) of the eCommerce Directive. The lack of proportionality in the scope of the filter together with concerns regarding the privacy of end-users led the CJEU to absolve Scarlet from implementing the measure sought by the rights holder (SABAM). The ruling is important for us in that it highlights the importance of Article 15 (1) in *limiting* copyright enforcement opportunities: ‘blanket’¹⁵⁴ monitoring of users is not tolerated in the EU, and any measure under Article 8 (3) of the EUIPD will be rendered unlawful if it amounts to general surveillance of end-users and networks, this being true even though the protection of IPRs is at stake, which is a legitimate concern. What seems clear from *Scarlet Extended* is that far-reaching enforcement measures, which are to apply to everyone indiscriminately, in contrast to being *targeted* measures directed towards identified infringers, are harder to satisfy proportionality requirements. For this reason, it is advisable for rights holders to keep the scope of enforcement requests always as *targeted* as possible, as the wider the implications

¹⁵⁴ The term refers to a measure which applies indiscriminately towards everyone and everything, in contrast to being targeted towards identified addressees.

of the measure sought are, the greater the risk of collateral damage becomes, and as a consequence, the more challenging it becomes to satisfy proportionality.

It also became clear from *Scarlet Extended* that orders which seek to compel ISPs to prevent infringements from *occurring* are harder to obtain than orders compelling them to address *existing* infringements, especially if rights holders are not able to pinpoint the (future) infringements. Blanket preventive measures rarely satisfy proportionality requirements, but more targeted preventive measures are not unlawful *per se*, and if the occurrence of a future infringement can be pinpointed in a reliable way, it may be appropriate to request for an order with preventive implications. Such injunctions are especially handy for rights holders looking to combat the illicit streaming of their live broadcasts. As the CJEU has affirmed that enforcement measures under the EUISD can be applied with a view to *prevent* infringements from occurring,¹⁵⁵ rights holders should not completely abstain from pursuing preventive enforcement strategies, but are advised to conduct rigorous proportionality evaluation with a view to ascertain that the measure sought satisfies the case-specific proportionality considerations.

7.1.4 *UPC Telekabel Wien*: a targeted enforcement strategy contributes to proportionality

In contrast to *Scarlet Extended*, the *UPC Telekabel Wien* case provides for a more sensible and targeted enforcement strategy, where the measure in question (website block)¹⁵⁶ regarded one specific web address (the German *kino.to*), a website which offered downloading and streaming services used by end-users to view unauthorised copyright protected content (mainly movies and shows).¹⁵⁷ In contrast to *Scarlet Extended*, the rights holders in *UPC Telekabel Wien* applied for a targeted measure (user-end website block) which would address the infringements occurring in *kino.to* specifically, instead of establishing general monitoring requirements. The CJEU ultimately sided with the copyright holders in accepting that *generic* blocking requests could be made against ISPs freedom to conduct business. Such generic requests leave ISPs a great deal of discretion, as they are left to chose the best solution for protecting copyright online and achieving the objective of

¹⁵⁵ Case C-70/10 *Scarlet Extended* [2011] ECR I-11959, at 31.

¹⁵⁶ The order required UPC to limit access of its customers to *kino.to* by blocking its domain name and (present) IP address, as well as any other IP address of the website which of UPC would become aware of.

¹⁵⁷ Judgment of 27 March 2014, *UPC Telekabel Wien* (C-314/12), EU:C:2014:192.

the block, which goes a long way to satisfy proportionality in respect of the ISPs right to conduct a business. In the case, the CJEU affirmed that the fundamental rights at stake do not preclude courts from being able to grant generic blocking orders against ISPs, provided that (1) such blocking does not unnecessarily deprive end-users from being able to access information available lawfully, and (2) such blocking at least seriously discourages end-users from accessing the subject-matter, if the complete prevention of access to protected content can not be achieved.¹⁵⁸

As generic blocking requests leave it to ISPs to decide what measure ought to be implemented with a view to achieve the objective of protecting copyright, the burden of evaluating proportionality of measures is essentially shifted from rights holders to ISPs. It must be reinstated here that ISPs, just like rights holders, are advised to always conduct proportionality evaluation when considering measures under Article 8 (3) of the EUIPD, as adequate balancing contributes to lawful implementation of copyright enforcement, which further helps the ISP in this case avoid disproportionality claims. It should be stated here that concerns regarding generic blocking requests do exist, the most prominent one being that, in theory, ISPs can make use of the opportunity to implement overly lax enforcement measures, with a view to safeguard themselves from becoming burdened by measures intended to protect copyright holders. While this concern has merit to it, it is highlighted here that the CJEU did provide that ISPs must take “*all reasonable measures*” in implementing generic blocking orders, and this “reasonableness requirement” affords rights holders some ground to challenge merely symbolic measures implemented by ISPs.¹⁵⁹

It is clear that targeted blocking is less like to have adverse effects on ISPs and end-users alike, as end-users are less like to be stripped from their rights by such blocking, and ISPs are less like to incur negative burdens when they actually know what the scope of a website block (or any other enforcement measure) is. It is submitted that with targeted enforcement strategies, the risk of collateral damage and fundamental rights conflicts becomes smaller, because such risks can be envisaged and addressed before moving on to the implementation phase. With respect to blanket measures, this is of course not the case, as such measures are by nature intended to apply generally towards everyone and everything, and so it becomes impossible (or extremely challenging at the

¹⁵⁸ Id, at 63.

¹⁵⁹ Id, at 64.

very least) to consider every single possible fundamental rights conflict that such a measure may give rise to. For this reason, rights holders are advised to prefer targeted measures over vague and all-reaching measures, as injunctions are more likely to be granted to rights holders who are able to pinpoint infringements and infringing actors, and further request for measures which specifically address infringements, in contrast to looking to establish burdensome general policing mandates to faultless ISPs.

7.2 Criteria used for assessing proportionality of website blocking injunctions

On a general note, it is submitted that the underlining proportionality consideration is that, the greater the adverse economic impact of the copyright violation is, the more potent enforcement measures should be available to rights holders looking to combat such infringements. Respectively, the greater the costs and burdens that blocking causes to ISPs, and the more the blocking limits the fundamental rights of parties involved, the more substantial the scale of the infringement, economic loss, and need to protect intellectual property must be in order for the blocking to be considered a proportionate way to tackle the infringements. It should be kept in mind that the criteria to be considered in assessing proportionality of website blocking injunctions are always case specific, and the following discussion cannot therefore *exhaustively* take account of all possible considerations which could be relevant in evaluating the proportionality of website blocking orders. Nevertheless, the following discussion does provide for an overall view of what a proportionate website block generally entails.

For an injunction under Article 8 (3) of the EU Infosoc Directive to satisfy proportionality requirements, there are several matters which should be addressed. The starting point is that, for a measure to be proportionate under EU law, its *aim* must be legitimate, it must be *suitable* to achieve the aim, and it must be *necessary* to achieve the aim, in addition to being *reasonable* in light of competing interests.¹⁶⁰ On top of these general proportionality remarks, balancing of rights often requires further case-specific considerations. In respect of website blocking injunctions, it is submitted that the following criteria may be used to determine whether a given website blocking

¹⁶⁰ P. Craig, G. de Burca, EU Law: Text, Cases, and Materials, OUP Oxford (5th ed.), at 526 (2011). In addition, Article 52 (1) of the EU Charter provides that the rights and freedoms recognised in the EU Charter can be restricted only when they satisfy the principle of proportionality.

request can be regarded as proportionate: the blocks *effectiveness* and *dissuasiveness* for its purposes, *substitutability* of the blocking measure, the availability of *less restrictive alternative measures*, the requirement that the blocking is *not unnecessarily complicated or costly*, and the existence of *safeguards* intended to keep the blocking as lawful as possible. We will discuss these remarks now with a view to address what such considerations entail.

7.2.1 Effectiveness

Considering the effectiveness of a website block is a crucial part of proportionality evaluation, and various studies have been conducted with regard to the effectiveness of website blocking.¹⁶¹ The problem is that such studies provide for varying and conflicting conclusions on the effectiveness of website blocking, and there is no political consensus on the efficiency of website blocking within the EU. To briefly illustrate this matter, certain Italian and Belgian studies, which have been used by rights holders to pave the way for website blocking mandates, provide that the effectiveness of website blocking falls between 73% - 80%, whereas on the other end, we have a widely-cited study conducted by the University of Amsterdam, which is more modest in providing that the effectiveness of website blocking ranges between 4 - 6%.¹⁶² In the authors opinion, the efficiency of website blocking probably ranks closer to the results of the Dutch study, mainly because end-users who recurrently engage in piracy activities already know various piracy platforms online, and when one site is blocked at the user-end, it easy for them to change to change to another website, find proxy services which allow access to the blocked website, or simply use a VPN service to bypass user-end blocking.¹⁶³ As recurrent pirates are more determined to engage in piracy then other end-users, its seems logical that circumventable blocking is less like to affect them. Still, website blocking has become increasingly more popular among rights holders copyright enforcement strategies, despite the fact that the effectiveness of such blocking remains a controversial matter. In advising the CJEU in *UPC Telekabel Wien*, AG Villalón noted that circumvention of user-end

¹⁶¹ P. Savola, “Proportionality of Website Blocking: Internet Connectivity Providers as Copyright Enforcers,” 5 JIPITEC 116, at para. 73 [2014].

¹⁶² For considerations regarding the studies referred to, *see*: P. Savola, “Proportionality of Website Blocking: Internet Connectivity Providers as Copyright Enforcers,” 5 JIPITEC 116, at para. 74 [2014].

¹⁶³ Finding proxy websites is extremely easy. Googling ‘TPB proxy’, for instance, gives rise to numerous proxy websites allowing access to TPB. Discussion regarding the liability of search engines is especially controversial, and cannot be included in this study.

blocks is a legitimate concern to rights holders,¹⁶⁴ but he also went on to provide that, in his opinion, the fact that certain users may circumvent website blocks does not go on to render website blocking inappropriate and inefficient as such,¹⁶⁵ and the author of this study must uphold this view of the AG, as it would seem too harsh to render the whole measure of website blocking inefficient without further political consensus on the matter. For the time being, the CJEU would seem to agree with the AG, as it confirmed in *UPC Telekabel Wien* that website blocks can be considered effective despite the fact that they can be circumvented, provided that such blocks serve to seriously discourage end-users from engaging in infringing activities.¹⁶⁶ What exactly qualifies as ‘seriously discouraging’ has been left open for interpretation, but it would seem that website blocking is often considered ‘efficient enough’ for its purposes. Although the author of this thesis recognises that inefficient measures, which have merely symbolic function, should not be the preferable mean for rights holders to protect and enforce their rights, the author would also like to highlight that, in the digital environment, there will probably never be a *perfect* solution to combat piracy, and so it would seem unreasonable to deny rights holders protection on grounds that the enforcement strategy they pursue does not address the infringements in a perfect way. Consequently, it is submitted that, for the time being, until further technical and political consensus on the efficiency of website blocking is reached in the EU, rights holders are advised to include such blocking as part of their copyright enforcement strategy, if they sincerely believe that the implementation of such blocking would have the effect of at least seriously discouraging end-users from engaging in piracy.

7.2.2 Subsidiarity

Subsidiarity is the next proportionality consideration that ought to be addressed. Website blocking at the user-end is not always the most proportionate way to combat piracy, as other intermediaries may at times be better placed to combat infringements directly at the source, which makes pursuing action against ISPs disproportionate. In particular, website *hosting* service providers may be compelled to refrain from hosting unlawful websites. Certain authors advocate that piracy should first and foremost be addressed at the source in this way, and only when absolutely necessary, at the

¹⁶⁴ The Opinion of AG Villalón in *UPC Telekabel Wien* (Case C-314/12) ECLI:EU:C:2013:781, at 99.

¹⁶⁵ *Id.*, at 100.

¹⁶⁶ Case C-314/12 *UPC Telekabel Wien* [2014], EU:C:2014:192, at 63.

user-end, through ISPs.¹⁶⁷ Initially, this would seem to make sense — it seems unfair that faultless ISPs should be required to act when there is the real possibility of addressing infringements directly at the source, thus putting a more *final* end to the infringements. However, as noted before in this study, piracy website operators are not like to be collaborative in putting an end to their services. It is submitted here that blocking at the user-end becomes the more appropriate way to combat anonymously remaining bad faith website operators, especially if there is evidence indicating that such operators have repeatedly changed hosting providers following legal attempts to take them down at the source. If it was otherwise, combating unlawful websites would become a global game of cats-and-mice between rights holders and pirates, something which becomes frustrating and expensive to pursue, especially since there is no guarantee that such enforcement attempts will lead to successful compensation of infringements, or even the termination of the websites operation. Still, a certain percent of piracy website operators may terminate their functioning completely upon being denied hosting services following enforcement measures taken against them, but with regard to the established and more notorious pirate sites — the ones which contribute to the piracy ecosystem the most — it is likely that such operators will simply change hosting providers and return to their ordinary functioning. It should be kept in mind that website operators who engage in unlawful doings are often registered and hosted overseas, in places like Panama and Costa Rica, where it can be very hard for rights holders to push through with their EU copyright enforcement agendas.

In light of the hardships associated with chasing website operators who simply change hosting providers upon being taken down at the source, it is proposed here that the subsidiarity requirement can be satisfied especially when dealing with website operators who do not operate in a *bona fide* manner. The lack of such good faith becomes apparent when considering, *inter alia*, the *intent* of the websites services, the *design* of the website, the websites *responsiveness* to contact efforts from the side of rights holders, the extent to which the website *collaborates* with rights holders in limiting the scale of infringements occurring through the website, and the levels of *infringing activities* that take place through the website. Further, if in addition to the above considerations it

¹⁶⁷ A. Lodder, N. van der Meulen, “Evaluation of the Role of Access Providers: Discussion of Dutch Pirate Bay Case Law and Introducing Principles on Directness, Effectiveness, Costs, Relevance, and Time,” 4 JIPITEC 130, at 71 [2013].

becomes apparent that a website operator is making economic gain in operating the website which contributes to piracy, rights holders can conclude that the operator can not be considered a *bona fide* service provider. Here, it becomes more appropriate and necessary to deal with the website at the user-end, and subsidiarity may be consequently satisfied.

7.2.3 Availability of less restrictive alternative means

The availability of *less restrictive alternative means* is an important part of proportionality evaluation in website blocking cases. Alternative measures to combat piracy pertaining in websites do exist, and sometimes, such measures may constitute more appropriate and less restrictive means to combat piracy pertaining in the web. However, it can be argued that alternative means less potent than website blocks are inefficient for the purposes of combating piracy. The problem with anything less potent than a website block is that such a measure often requires *bona fide* collaboration from the side of website operators in order to function as intended. When dealing with *bona fide* website operators, less restrictive measures than website blocks can give rise to successful outcomes, this is not denied, but for the purposes of combating established bad faith piracy websites, such measures based on mere goodwill of the website operator are undoubtedly useless for the purposes of protecting IPRs. For example, takedown notices, *i.e.* the practice where rights holders make extensive efforts to send requests to websites contributing to piracy, asking them to stop doing so, are more or less completely ignored by websites who do not operate under *bona fide* terms. It seems only logical that any measure requiring *bona fide* collaboration from the side of a *non-bona fide* operator amounts to an inefficient way to combat copyright infringements pertaining through the website, as bad faith piracy websites are not like to suddenly stop contributing to the piracy ecosystem upon receiving a friendly letter from rights holders asking them to do so.

Albeit it is true that established and notorious piracy websites are like to ignore *bona fide* requests to address infringing activities pertaining through their services, rights holders are advised *never* to take this for granted, but rather, they are advised to show upon applying for an injunction that they have indeed made extensive efforts to contact such websites with a view to ask them to put an end to violations of copyright. Upon application for an injunction, rights holders are advised to include any evidence indicating that the bad faith nature of the website. Once this is done, it becomes more

convenient for the relevant authority to accept that anything less potent than the sought website block would amount to an inefficient way to tackle the infringements, and the chances of being granted the injunctive relief sought becomes thus higher.

7.2.4 Implementation costs

In website blocking, the copyright holder essentially shifts the burden of protecting copyright to ISPs, and it has often been the case that ISPs have further been ordered to assume the costs of implementation.¹⁶⁸ EU law does not explicitly regulate who is to assume implementation costs, and this has been dealt with differently in the Member States of the EU.¹⁶⁹ The author of this study would like to highlight that, if copyright holders were required to at least *contribute* to implementation costs, it would likely make them conduct more rigorous proportionality evaluation before moving on to request for injunctive relief, which would likely then have a positive effect on the quality of injunctions granted to rights holders, as well as the amounts of injunctions granted to such rights holders. Further, sharing implementation costs has the effect of paving the way for a more mutual relationship between rights holders and ISPs, who are becoming increasingly more involved with one another. A system of dual financing would be beneficial to rights holders also, as ISPs would surely be more enthusiastic about collaborating with rights holders and protecting their copyright, if assured that they will not be required to assume implementation costs solely by themselves. This would probably also result in a decrease in how often ISPs challenge measures sought by rights holders, and consequently, the enforcement and protection of copyright would not be hindered by on-going litigation.

However, since implementation costs in this context have not been explicitly regulated at the EU level, the previous observations amount to merely food for thought for the time being. What can be said with certainty is that, the more symbolic a measure under Article 8 (3) of the EUIPD is in terms of its efficiency, the more disproportionate it is to require ISPs to assume implementation costs; respectively, the more efficient a measure is for the purposes of protecting copyright, the less like it

¹⁶⁸ M. Husovec, “Injunctions against Innocent Third Parties: The Case of Website Blocking”, 4 JIPITEC 116, at 47 [2013].

¹⁶⁹ K. Fox, J. Jones, “Getting the look for less? The blocking cost: Cartier International v BSKyB (Court of Appeal)”, E.I.P.R. 2017, 39(1), 58-65, at 64 [2017].

is for costs of implementation to become the reason why a website blocking request is deemed disproportionate.

7.2.5 Safeguards

Finally, when requesting an injunctive order from the court, it is advisable for rights holders to consider whether the order sought could be accompanied by case-specific *safeguards* designed to minimise the adverse effects and burdens of the order sought. It makes sense that injunctions accompanied by safeguards intended to protect the addressee ISPs add on to the proportionality of such measures, and rights holders are always advised to consider whether safeguards could be put in place with a view to help keep their enforcement request lawful, as this betters their chances of receiving the relief sought. An example of such a safeguard could be an expiring duration-limit on a website blocking order, which would require the addressee ISP to implement blocking only for a specified duration of time, when the infringements are like to occur. This kind of a safeguard is especially suitable for the purposes of blocking the unauthorised streaming of live broadcasts of sports events, as became apparent in the *Premier League* case discussed before. It is submitted here that safeguards go a long way to add on to the proportionality of injunctive relief requests, and rights holders are advised to include such safeguards whenever possible and appropriate to do so.

7.3 Interim conclusions

We have now examined the role of proportionality evaluation in website blocking injunctions, and further highlighted criteria which contribute to lawful application of Article 8 (3) of the EUIPD. As has become evident, proportionality evaluation is of pivotal importance when looking to arrive to a well-balanced and a lawful order. As ISPs are faultless intermediaries, and as their functioning is neutral and purely technical, enforcement measures against them must remain proportionate, as ISPs do not encourage consumers to engage in unlawful activities, but rather, their services are abused by consumers looking to partake in different modes of piracy. The importance of proportionality evaluation has been further affirmed by the CJEU, who has provided that the protection of IPRs is not absolute, but rather, it must be balanced with other competing interests.¹⁷⁰ For the time being, website blocking would seem to be a useful strategy to combat piracy. Although

¹⁷⁰ Judgment of 27 March 2014, *UPC Telekabel Wien* (C-314/12), EU:C:2014:192, at 61.

the efficiency of the measure remains controversial today, in the absence of reliable data on the efficiency of website blocking, rights holders are advised to pursue such blocking against piracy facilitating websites and online platforms, provided that they sincerely accept that such blocking has the effect of providing them immediate relief from pertaining infringements, and provided that such measures do not have merely symbolic function, but actual copyright protecting and infringement-mitigating implications. Rights holders are hereby advised never to lose sight of the importance of proportionality evaluation, as proportionality evaluation is pivotal in determining the legality of measures under Article 8 (3) of the EUIPD.

8. Conclusion

The research has been conducted and it is time to address the research questions. It was first asked, what is the role of ISPs in the piracy schemes, and to what extent can measures under Article 8 (3) of the EUIPD be used to compel such ISPs to collaborate with rights holders piracy-combating enforcement strategies. It has been affirmed by the CJEU that ISPs qualify as intermediaries under Article 8 (3), and therefore, they are subject to injunctions where their services are used by third-parties (consumers) to partake in copyright infringements. However, due to the technical and neutral functioning of ISPs, the extent to which enforcement against them is lawful largely depends on the proportionality of measures against them — enforcement measures must be balanced, meaning that they must take account of the competing interests, and further strike a balance between such interests, in a way that reflects the scale of the infringements in question, and does not overly burden ISPs, as they have the right to conduct a business. Thus, the extent to which ISPs may be compelled to implement enforcement measures under Article 8 (3) is a matter of *proportionality*, which bring us to our second research question.

The second research question asked what proportionality considerations are important when looking to implement a lawful enforcement strategy against ISPs under Article 8 (3) of the EUIPD. For measures under Article 8 (3) of the EUIPD to satisfy proportionality requirements, there are several matters which should be addressed. The basic starting point is that the measure sought must: (1) have a legitimate aim, (2) be suitable for achieving the aim, and (3) be necessary to achieve the aim. Whether these are satisfied, it can be determined by carefully examining the case-specific trade-offs of the request, as well as the possible future impacts of granting the injunction. It was noted that although what constitutes proportionality may be specified at the national level, such considerations can hardly be codified in an exhaustive manner, as proportionality generally requires case-specific balancing considerations. The case law of the CJEU is helpful in determining the legality of measures under Article 8 (3), as the said court has provided for guidelines and constraints on the application of measures under Article 8 (3). From such case law, we learned that, *inter alia*, Article 15 (1) of the eCommerce Directive has significant implications in limiting enforcement strategies, as all measures constituting ‘blanket monitoring’ will be rendered unlawful under EU law, even though such measures have the objective of protecting IPRs online. It also became clear that

targeted measures are more likely to satisfy proportionality requirements, as such measures enable rights holders and courts alike to address the effects of the measures sought if implemented, after which it becomes easier to determine whether the measure sought can be considered lawful and proportionate. It is proposed that rights holders should keep their enforcement strategy as *targeted* as possible, as the more vague the scope of the measure applied for is, the greater the risk of collateral damage becomes, and consequently, the harder it becomes to satisfy proportionality requirements. It is also proposed that rights holders should attempt to incorporate safeguards into measures under Article 8 (3) of the EUIPD, as such safeguards go a long way to highlight the *bona fide* nature of the injunctive relief request, and consequently, such safeguards greatly contribute to the lawfulness of enforcement measures under Article 8 (3).

Importantly, measures under Article 8 (3) of the EUIPD should be: *effective and dissuasive* for their purposes, rather than merely symbolic; there should be *no less restrictive alternative means* suitable for the purposes of combating infringements, as this would go on to render the measure sought unnecessary; measures should not be unnecessarily *costly* or entail *overly burdening obligations* on ISPs, who are faultless intermediaries; measures should not amount to *over-blocking*, as this would give rise to fundamental rights concerns; measures should satisfy *subsidiary* requirements, and be targeted towards ISPs only when combating infringements at the source is clearly not efficient for the purposes of protecting copyright; and finally, measures should include *adequate safeguards* whenever possible, as such safeguards go on to show that rights holders are not trying to dominate ISPs and other parties with their enforcement strategies, but rather, that they are sincerely trying to protect their exclusive rights, and restrict their enforcement attempts to what is strictly needed in order to achieve the objective sought (protection of copyright). The underlying proportionality consideration in measures under Article 8 (3) is that such measures must be balanced and adequately envisage and limit adverse effects to affected parties' rights and freedoms. Overly restrictive measures, as well as merely symbolic measures, are not likely to pass proportionality analysis, as injunctions need to strike a balance between competing interests, and remain suitable for the purposes of protecting copyright.

It is submitted here that the EU legal framework *does* provide for a high level of legal protection against copyright piracy, but what is needed is rigorous application of such laws by national courts,

and motivation to enforce rights by rights holders. Proportionality evaluation is *key* in determining the lawfulness of injunctions under Article 8 (3) of the EUIDS, and rights holders should always try to formulate their requests in a manner which can satisfy proportionality tests.

Summary

This thesis, which adopts a law & technology perspective in researching the legal problem of copyright piracy, aims at examining the extent to which injunctions under Article 8 (3) of the Directive 2001/29/EC can be used by rights holders to compel internet service providers to combat copyright piracy online. Article 8 (3) of the Directive 2001/29/EC requires Member States of the EU to make sure that copyright holders can apply for injunctions against intermediaries whose services are used by third-parties to infringe copyright, and it has been affirmed by the CJEU that ISPs qualify as intermediaries under Article 8 (3).

Throughout the thesis, there is a constant emphasis on EU law. The study analyses how the CJEU has interpreted Article 8 (3) of the Directive 2001/29/EC, and further makes use of such CJEU-provided insight in highlighting the elements that contribute to lawful implementation of Article 8 (3) of the Directive 2001/29/EC. Because Article 8 (3) of the Directive 2001/29/EC does not come with guidelines on its correct application, the preliminary rulings of the CJEU are an extremely important source of information on the application of the said provision, as such rulings enable us to conclude how rights holders may arrive to lawful measures and a lawful copyright enforcement strategies under Article 8 (3) of the Directive 2001/29/EC.

Ultimately, it is concluded that proportionality of measures is *key* in determining the legality of injunctions against internet service providers under Article 8 (3) of Directive 2001/29/EC, and that rights holders need to conduct rigorous evaluation of enforcement measures sought in order to make sure that their injunctive relief requests will be upheld by courts. The study makes proposals regarding rights holders enforcement strategies against internet service providers, as well as remarks regarding the future of ISPs and copyright enforcement. The underlying consideration is that, the more symbolic and restrictive a measure sought under Article 8 (3) of the Directive 2001/29/EC is, the harder it is to satisfy proportionality requirements; respectively, the more efficient and limited a measure sought is, the more likely it is that such an injunctive request will be upheld and deemed proportionate in light of the objective of protecting copyright.

Oversigt

Denne afhandling, der vedtager et lov- og teknologiperspektiv ved undersøgelsen af det juridiske problem vedrørende piratkopiering af ophavsret, sigter mod at undersøge, i hvilket omfang forbud i henhold til Artikel 8 (3) i Direktiv 2001/29/EC kan benyttes af rettighedshavere til at tvinge internettet Tjenesteydere til at bekæmpe piratkopiering af ophavsret online. I henhold til Artikel 8 (3) i Direktiv 2001/29/EC skal EU's medlemsstater sørge for, at indehavere af ophavsret kan anmode om påbud mod formidlere, hvis tjenester anvendes af tredjeparter til krænkelse af ophavsret, og det er bekræftet af Domstolene, at internetudbydere kvalificerer sig som formidlere i henhold til Artikel 8 (3).

I hele afhandlingen er der konstant fokus på EU-lovgivningen. Undersøgelsen analyserer, hvordan EU har fortolket Artikel 8 (3) i Direktiv 2001/29/EC, og yderligere gør brug af en sådan domstol gav indsigt i at fremhæve de elementer, der bidrager til lovlige gennemførelse af Artikel 8 (3) i Direktiv 2001/29/EC. Da Artikel 8 (3) i Direktiv 2001/29/EC ikke indeholder retningslinjer for den korrekte anvendelse, er de præjudicielle afgørelser fra den portugisiske regering en yderst vigtig kilde til oplysninger om anvendelsen af nævnte bestemmelse, da sådanne afgørelser gør det muligt for os At konkludere, hvordan rettighedshavere kan komme til lovlige foranstaltninger og lovlige ophavsretlige håndhævelsesstrategier i henhold til Artikel 8 (3) i Direktiv 2001/29/EC.

I sidste ende konkluderes det, at proportionaliteten af foranstaltninger er afgørende for at fastslå lovligheden af forbud mod internetudbydere i henhold til a Artikel 8 (3) i Direktiv 2001/29/EC, og at rettighedshavere skal foretage en streng vurdering af For at sikre sig, at deres anmodninger om forbud mod afhjælpning vil blive opretholdt af domstole. Undersøgelsen indeholder forslag til rettighedshaveres håndhævelsesstrategier over for internetudbydere, samt bemærkninger vedrørende fremtidens internetudbydere og håndhævelse af ophavsret. Den underliggende overvejelse er, at jo mere symbolsk og restriktive en foranstaltning er søgt i henhold til Artikel 8 (3) i Direktiv 2001/29/EC, desto sværere er det at opfylde proportionalitetskravene. Den desto mere effektive og begrænsede en foranstaltning er, desto mere sandsynlig er det, at en sådan forbudsbegydelse vil blive opretholdt og anses for proportional i lyset af formålet med at beskytte ophavsret.

Bibliography

Official Documents

International

Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). The TRIPS agreement is Annex 1C to the Marrakesh Agreement Establishing the World Trade Organisation, done at Marrakesh on the 15th April 1994, 33 I.L.M. 1125.

European Union

The Charter of Fundamental Rights of the European Union (2000/C364/01).

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 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.

Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

European Commission, "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," SEC(2010) 1589 final.

Other

OFCOM, "Online copyright infringement tracker benchmark study Q3 2012: Introduction and Key Findings," [2012].

Frontier Economics, “The Economic Impacts of Counterfeiting and Piracy: Report prepared for BASCAP and INTA,” [2016].

Study conducted by the European Union Intellectual Property Office, “The Economic Cost of IPR Infringement in the Recorded Music Industry,” May 2016.

A joint project between Europol and the European Union Intellectual Property Office, “2017 Situation Report on Counterfeiting and Piracy in the European Union”, June 2017.

Case Law

European Court of Human Rights

Fredrik Neij and Peter Sunde Kolmisoppi (The Pirate Bay) v. Sweden, Appl. nr. 40397/12; ECLI:CE:ECHR:2013:0219DEC004039712.

Court of Justice of the European Union

Case C-275/06, Productores de Música de España (Promusicae) v Telefónica de España SAU, Judgment of the Court (Grand Chamber), 29 January 2008.

C-557/07, LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH, Order of the Court (Eighth Chamber), 19 February 2009.

Case C-70/10, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), Judgment of the Court (Third Chamber), 24 November 2011.

C-314/12, UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH, Judgment of the Court (Fourth Chamber), 27 March 2014.

C-527/15, Stichting Brein v Jack Frederik Wullems, Judgement of the Court (Second Chamber), 26 April 2017.

Case C-610/15, Stichting Brein v Ziggo BV, XS4ALL Internet BV, Judgement of the Court (Second Chamber), 14 June 2017.

National EU Member States

Stockholm's District Court (*Tingsrätt*) ruling in case B 13301-06.

IFPI Denmark v Tele2 A/S, Case F1-15124/2006, 25 October 2006 (City Court of Copenhagen).

Sonofon A/S v. IFPI Denmark, Case 153/2009, 27 May 2010 (Supreme Court of Denmark).

Twentieth Century Fox Film Corp & Ors v British Telecommunications Plc [2011] EWHC 1981 (Ch) (28 July 2011).

Football Association Premier League Ltd v British Sky Broadcasting Ltd & Ors [2013] EWHC 2058 (Ch) (16 July 2013).

Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors [2014] EWHC 3354 (Ch) (17 October 2014).

Swefilmer, Swedish Court of Patent Appeals and the Market Court, case 11706-15 (2017).

Football Association Premier League Ltd v British Telecommunications Plc & Ors [2017] EWHC 480 (Ch) (13 March 2017).

United States of America

Sony Corporation v. Universal City Studios, Inc., 464 U.S. 417 [1984]

A&M Records Inc v Napster, Inc 114 F. Supp 2d 896 [2000].

Other

Opinion of Advocate General Cruz Villalón in UPC Telekabel Wien (Case C-314/12) ECLI:EU:C:2013:781.

Opinion of Advocate General Maciej Szpunar in *Stichting Brein* (Case C-610/15) ECLI:EU:C:2017:99.

Books

M. Einhorn, "Media, Technology and Copyright: Integrating Law and Economics," Edgar Elgar Publishing Inc., at 79 [2004].

N. Reich, "Understanding EU Law: Objectives, Principles and Methods of Community Law," Intersentia Publishing [2005].

K. Sideri, "The regulation of Peer-to-Peer Sharing Networks: Legal Convergence v. Perception Divergence", *in* F. Macmillan (ed.), "New Directions in Copyright Law", Edward Elgar Publishing Inc, [2005].

S. Stokes, "Digital Copyright, Law and Practice," Hart Publishing [2005].

R. Haynes, "Media Rights and Intellectual Property," Capstone [2005].

G. Mazziotti, "EU Digital Copyright Law and the End-User," [2008].

S. Stokes, "Digital Copyright: Law and Practice", Hart Publishing [2009].

D. Kioupis, "Criminal Liability on the Internet", *in* I. Stamatoudi (ed.), "Copyright Enforcement and the Internet", Kluwer Law International Publishing, at 241 [2010].

L. Gelsthorpe, "Copyright infringement: a criminological perspective", *in* J. Ginsburg (ed.), J. Davis (ed.), L. Betnly (ed.), "Copyright and Piracy: an Interdisciplinary Critique", Cambridge University Press Publishing [2010].

Paul Craig, Gráinne de Búrca, "EU Law: Text, Cases, and Materials," OUP Oxford (5th ed.) (2011).

W. Patry, "How to Fix Copyright," Oxford University Press [2012].

T. Cvetkovski, "Copyright and Popular Media, Liberal Villains and Technological Change" [2013].

J. Griffiths, L. McDonagh, "Fundamental Rights and European IP law: the case of Art 17 (2) of the EU Charter", in C. Geiger (ed.), "Constructing European Intellectual Property: Achievements and New Perspectives," European Intellectual Property Institutes Network series [2013].

P. Savola, "Internet Connectivity Providers as Involuntary Copyright Enforcers: Blocking Websites in Particular," University of Helsinki, Publications of IPR University Center, [2015].

Articles

O. Pavlov, "Dynamic Analysis of an Institutional Conflict: Copyright Owners Against Online File Sharing," *Journal of Economic Issues*, v.39 (3) [2005].

R. Giblin-Chen, "Rewinding Sony: an inducement theory of secondary liability," *E.I.P.R.* 27(11) [2005].

Joel Smith, "European Community: copyright - data privacy does not trump copyright protection," *E.I.P.R.* 30(6) N39 [2008].

H. K. Larusson, "Uncertainty in the scope of copyright: the case of illegal file-sharing in the UK," *E.I.P.R.* 31(3) 124 [2009].

J. Reyman, "The Rhetoric of Intellectual Property Law, Copyright Law and the Regulation of Digital Culture," Routledge [2010].

P. Akester, "The new challenges of striking the right balance between copyright protection and access to knowledge, information and culture," *E.I.P.R.* 32(8) 372, [2010].

U. Kohl, "The rise and rise of online intermediaries in the governance of the Internet and beyond – connectivity intermediaries," 26 *IRLCT* [2012].

P. Torremans, "Copyright Territoriality in a Borderless Online Environment" in J. Axhamn (ed.), *Copyright in a Borderless Online Environment*, [2012].

A. Stazi and D. Mula, "Intellectual Property and Consumer Law" in A. Ramalho (ed.), "Crossroads of Intellectual Property, Intersection of Intellectual Property and other Fields of Law," [2012].

D. Meale, "SABAM v Scarlet: of course blanket filtering of the internet is unlawful, but this isn't the end of the story," E.I.P.R. 34(7) [2012].

J. Blevins, "Uncertainty as Enforcement Mechanism: The New Expansion of Secondary Copyright Liability to Internet Platforms", 34 Cardozo Law Review, Loyola University New Orleans College of Law Research Paper 2013-12 [2013].

M. Husovec, "Injunctions against Innocent Third Parties: The case of Website Blocking," 4 JIPITEC, 2 [2013].

A. Lodder, N. van der Meulen, "Evaluation of the Role of Access Providers: Discussion of Dutch Pirate Bay Case Law and Introducing Principles on Directness, Effectiveness, Costs, Relevance, and Time," 4 JIPITEC 130 [2013].

M. Daly, "Is there an entitlement to anonymity? A European and international analysis", E.I.P.R., 35(4), 198 - 211 [2013].

S. Liebowitz, "The impact of internet piracy on sales and revenues of copyright owners," an abridged version of the full paper: "Internet piracy: the estimated impact on sales", in Handbook on the Digital Creative Economy, Edited by R. Towse and C. Handke, Edward Elgar [2013].

H. Schulze and K. Mochalski, "Internet Study 2008/2009," Technical Report, Ipoque GmbH, 2009 in EPFIA: Extensible P2P Flows Identification Architecture, Journal of Applied Mathematics and Physics, [2013].

Kevin T. O'Sullivan, "Enforcing copyright online: internet service provider obligations and the European Charter of Human Rights", E.I.P.R. [2014]

P. Günther, M. Norrgård, "Blocking Websites: Copyright Enforcement Online and Responsibilities of Internet Intermediaries in Europe", JFT 3/2014 s. 97–131 [2014]

Pekka Savola, "Proportionality of Website Blocking: Internet Connectivity Providers as Copyright Enforcers," 5 JIPITEC 116, [2014].

P. Günther, "The plan for a digital Single Market in Europe and reforming EU copyright rules to develop a market-oriented approach to reduce infringement on the internet," E.I.P.R. 38(1) [2016].

A. Roy, A. Marsoof, "The blocking injunction: a comparative and critical review of the EU, Singaporean and Australian regimes," E.I.P.R. 38(2) [2016].

S. Baggs, R. Alexander, E. Preston, "Curtains down on Popcron Time: s.97A takes centre stage," E.I.P.R. 38(1), [2016].

B. Jütte, "The beginning of a (happy?) relationship: copyright and freedom of expression in Europe", E.I.P.R. 38(1), 11 - 22 [2016]

E. Rosati, "Why a reform of hosting providers' safe harbour is unnecessary under EU copyright law", E.I.P.R. 38(11), 668 - 676 [2016]

P. Letai, "Don't think twice, it's all right: toward a new copyright protection system", E.I.P.R. 37(12), 765-772 [2016]

Dr. Clark, S. Tozzi, "Communication to the public under EU copyright law: an increasingly Delphic concept or intentional fragmentation?", E.I.P.R. 38(12), 715-717 [2016]

K. Fox, J. Jones, "Getting the look for less? The blocking cost: Cartier International v BSKyB (Court of Appeal)", E.I.P.R. 2017, 39(1), 58-65 [2017]

M. Sag, J. Haskell, "Defense Against the Dark Arts of Copyright Trolling," Iowa Law Review [2017]

Websites

<http://www.bittorrent.com/company/about>

<http://rettighedsalliancen.dk/om-os/>

<https://torrentfreak.com/the-pirate-bay-must-be-blocked-in-sweden-court-of-appeal-rules-170213/>

<https://torrentfreak.com/hold-isps-responsible-for-piracy-after-brexit-music-biz-says-170512/>

<https://torrentfreak.com/streaming-site-operator-jailed-for-three-years-after-landmark-trial-170516/>

Danish Code of Conduct: <http://www.teleindu.dk/wp-content/uploads/2014/10/TI-code-of-conduct-blokeringer.pdf>

B. King, "The Day the Napster Died" [2002]. <https://www.wired.com/2002/05/the-day-the-napster-died/?currentPage=all>

Maria Fredenslund, "Denmark: Code of Conduct on website blocking," RettighedsAlliancen, (2014). Available here: <http://kluwercopyrightblog.com/2014/10/24/denmark-code-of-conduct-on-website-blocking/>.

The Local, "Swedish broadband provider must block The Pirate Bay, court rules," 13 February 2017. <https://www.thelocal.se/20170213/swedish-broadband-provider-must-block-the-pirate-bay-court-rules>

C. Cooke, "Major Swedish ISP says it won't web-block without a court order," 22 February, 2017. <http://www.completemusicupdate.com/article/major-swedish-isp-says-it-wont-web-block-without-a-court-order/>

E. Rosati, "Filmspeler, the right of communication to the public, and unlawful streams: a landmark decision", 27 April 2017. ipkitten.blogspot.fi/2017/04/filmspeler-right-of-communication-to.html

TorrentFreak, BREIN 'Hunts Down' Pirate Media Player Vendors. May 12, 2017. <https://torrentfreak.com/brein-hunts-down-pirate-media-player-vendors-170512/>