S(h)ifting the Cyberspace

Searching for effectiveness and human rights balance in the realm of online enforcement schemes aimed at digital content infringing copyright, trademarks, privacy or reputation.

Krzysztof Garstka

Thesis submitted to the

University of Nottingham

for the Degree of Doctor of Philosophy

April 2016

Table of Contents

Contents

Introduction.....5

Chapter 1 – Defining „infringing content" within the EU and UK legal frameworks.....9

1. Introduction.....9
2. Copyright-infringing content.....11
   2.1. European Union's legal framework governing the identification of copyright-infringing content.....11
   2.2. Factual scenarios leading to the transfer of copyright-infringing content.....17
3. Trademark-infringing content.....43
   3.1. European Union's legal framework governing the identification of trademark-infringing content.....43
   3.2. Factual scenarios leading to the transfer of trademark-infringing content.....45
4. Privacy-infringing content.....47
   4.1. European Union's legal framework governing the identification of privacy-infringing content.....47
   4.2. Factual scenarios leading to the transfer of privacy-infringing content.....51
5. Defamatory content.....58
   5.1. Legal framework of England and Wales governing the identification of defamatory content.....58
   5.2. Factual scenarios leading to the transfer of defamatory content.....59

Chapter 2 - Enforcement schemes aimed at the removal of access to infringing content.....65

1. Introduction.....65
2. Enforcement schemes focused on the infringers.....67

2.1. Subjecting the infringers to civil liability. 68
2.2. Subjecting the infringers to criminal liability. 75
2.3. Identifying the infringers. 82
2.4. Graduated response schemes. 85
2.5. Digital Rights Management. 88
3. Enforcement schemes focused on the intermediary. 91
3.1. Subjecting the intermediaries to civil liability. 92
3.2. Subjecting the intermediaries to criminal liability. 137
3.3. Limitations on intermediary liability. 143
Chapter 3 – Enforcement schemes' effectiveness. 154
1. Introduction 154
2. Primary areas of concern. 157
2.1. Renewal of access to infringing content (on a single platform). 158
2.2. Movements towards the alternative sources of infringing content. 161
2.3. Circumvention of the technological aspects of the enforcement schemes. 170
3. Deterrence effect of the enforcement schemes. 179
3.1. Deterring infringers. 179
3.2. Deterring intermediaries. 186
4. Diminishing returns of the enforcement schemes. 192
5. Social acceptance of infringing content. 195
Chapter 4 – The human rights implications of the enforcement schemes' activity. 202
1. Introduction. 202
2. The relevant human rights. 203
2.1. The right to property. 205
2.2. The right to respect for private and family life. 207
2.3. The freedom of expression and information. 210
2.4. The freedom to conduct a business. 214
2.5. The right to an effective remedy and to a fair trial. 215

3. Balancing the involved human rights. 217
3.1. The four protected interests vs the right to respect for private and family life. 218
3.2. The four protected interests vs the freedom of expression and information. 226
3.3. The four protected interests vs the freedom to conduct a business. 244
Chapter 5 – Towards the "specified request" model of intermediary liability. 252
1. Introduction. 252
2. Specified request vs blunt expectation: the two approaches to intermediary liability. 253
2.1. Description of both approaches. 253
2.2. Which approach to intermediary liability is conceptually better? .. 255
2.3. Requests which could be made of various involved intermediaries. 260
2.4. Implementing the specified request approach within the EU. 308
Bibliography 315

Introduction

With the development of cyberspace, mankind's ability to exchange tremendous amounts of information reached astonishing and praise-worthy levels. Unfortunately, such information also includes digital content infringing a variety of legitimate interests, such as copyright, trademarks, privacy, and reputation. Despite the increased regulatory activity of governments from all over the world, aimed at developing adequate legal frameworks governing the removal of access to such content, there are still significant concerns over the performance of this particular branch of online enforcement policy; concerns such as lack of effectiveness, or the impact of the endorsed solutions on the human rights framework.

The following thesis is aimed at responding to those concerns, from the perspective of the European Union's law. The work's overarching aim is to devise the most adequate, pan-European legal framework governing the removal of access to online content which infringes copyright, trademarks, privacy or is defamatory in nature. While those four content types differ from one another, this project delivers additional value by discovering such differences (as well as similarities) in the enforcement context, and taking them into account in its analysis and recommendations. The path towards attaining the thesis' research objective is drawn through the following five chapters.

The first chapter begins by gathering and organising the legal provisions which, if broken, can mark a piece of digital content as one infringing copyright, trademarks, privacy or reputation. The said provisions are then applied to a wide array of factual scenarios in which the described types of infringing content appear in cyberspace. It should be noted that the thesis draws in this context primarily on the EU law; where this is not possible, the

UK law is relied on. This is justifiable by the project's focus on the enforcement schemes, not on the definitions of infringing content.

The second chapter lays out the vast landscape of enforcement schemes endorsed within the EU for the purpose of removing access to the four chosen types of infringing content, both directly and indirectly. Such schemes are divided on those focused on the infringers themselves, and those focused on the intermediaries whose services are used for facilitating the transfer of infringing content. The chapter can be seen as laying out all the tools from the (regulatory) toolbox before deciding which ones to use - or alterate - for the task at hand.

The third chapter is the first of the two key, critically analytical chapters; it seeks to uncover and analyse the main challenges tied to the enforcement schemes' effectiveness. To this end, it begins by analysing three primary concerns of this kind; the renewal of access to infringing content (on a single platform), movements towards the alternative sources of infringing content, and circumvention of the enforcement schemes' technological aspects. This is followed by the analysis of the deeper effectiveness-related concerns (which often underlie the primary ones). They include the lack of deterrence, the notion of diminishing returns and the issue of social acceptance of infringing activities.

The fourth chapter explores the human rights implications of the enforcement schemes, with attention given to the balance struck within the EU law between the human rights protected by the said schemes, and those impaired by them. This is attained through two subchapters; the first one introduces the human rights involved and defines their scope, while the second discusses the enforcement schemes' impact on the three most affected human rights – the right to privacy, the freedom of expression and the freedom to conduct a business.

The conclusive, fifth chapter builds on its predecessors and proposes a fundamental upheaval of the approach to intermediary liability within the EU law, an upheaval aimed at responding to the concerns identified in chapters three and four and improving the degree of legal certainty within this branch of online enforcement. The chapter contains a corresponding proposal for a major reform of the EU legal framework.

This thesis is supported by a mixture of legal research methods, the doctrinal method being the first one. It underlies chapters one and two, it is crucial for setting out the landscape of human rights and discussing their legal interactions in chapter four, and finally, it plays an important role in devising and implementing the elements of the solution proposed in chapter five. For the second method, the thesis supports itself with qualitative and quantitative empirical studies; they provide evidence for the discussion of effectiveness in chapter three, and of the actual impact on human rights in chapter four. In both aspects, such studies provide (critically assessed) fuel for the conclusions in chapter five. The third method is the cross-disciplinary approach of law and technology – it plays a crucial role in the latter three chapters' analysis of interactions between regulatory measures and online technologies relevant to the thesis.

This doctoral project was funded by the University of Nottingham and Google UK, the latter of which acted as a collaborative research partner organisation. The thesis remains a result of the author's independent academic work.

The author would like to thank prof. Estelle Derclaye and prof. Paul Torremans for their invaluable, continuous support, as well as dr. Harjinder Obhi for his kind assistance throughout the project.

This thesis is dedicated to my family – my parents, Dorota and Jacek, my second half Karolina, and my little sister Ania. Thank you all for the support, belief, and patience: for lifting me up, while making sure that I keep my feet on the ground.

Chapter 1 – Defining „infringing content" within the EU and UK legal frameworks.

1. Introduction.

The purpose of this preliminary chapter is to discover and organise the current legal definitions of the "infringing content", a term used in this thesis to represent digital content regarded as infringing one of the four specific legitimate interests (namely copyright, trademark, privacy, and reputation (when damaged by defamatory content)). Before discussing the legal mechanisms and enforcement schemes adopted in order to remove access to infringing content, it is necessary to obtain a clear picture of various categories of digital content covered by this term.

In order to ensure the clarity of the distinction made between the first two chapters of this thesis, it should be underlined that chapter one goes only as far as the moment in which it is recognised that the act of transferring[1] a given category of digital content is regarded as an infringement of one of the four legitimate interests covered in this thesis. It does not, for example, cover the legal provisions making intermediaries liable for the infringing content; it is submitted in this thesis that such an approach is already an enforcement scheme in itself, aimed at the removal of access to the infringing content (even if it imposes primary liability on the intermediary.) While such a distinction might, seem slightly artificial at times, it is hopefully going to act as a reminder of the overarching aims of the discussed legal framework.

[1] Term to be understood broadly. The word transferring seems to be quite adequate in this context, for just as the Internet is made of the information flows, information which is not likely to be transferred to anyone does not, in principle, lead to infringement of the specified legitimate interests.

Another matter of artificiality which should be clarified upfront is the very concept of infringing content. One could be tempted to perceive it in a rather simplistic way, like a piece of information which by its very nature impairs a legitimate interest, no further questions needed. However, the reality is not as black and white, and the "infringing" label seems affixed far less firmly when we consider that a piece of seemingly infringing content might be covered by one of the available content type-specific defences or exceptions to infringement. For example, a video on Youtube containing a copyrighted music track, a video which seems like a clear-cut case of infringing content, might have been claimed by the copyright owner under YouTube's Content ID system,[2] or covered by the "fair use" defence[3] or some other copyright exception. Or a privacy-infringing post on a forum, containing the content of someone's emails, might turn out to be of sufficient public interest to remain accessible to the public. Nevertheless, the truth remains that infringing content does exist; and this thesis is focused on finding the most adequate response to this challenge. Consequently, while it does not deny the existence of exceptions and defences to infringement, it engages with them analytically only whenever the negative side effects of enforcement schemes are considered, impact on the freedom of expression in particular.[4]

A short note has to be made on the inclusion of the UK jurisdiction in this chapter. While the EU law harmonises (to a certain extent) the definitions of digital content infringing copyright, trademarks and privacy, it does not do the same with regards to defamatory content.[5] Nevertheless, in the Member States' jurisdictions, defamatory content is being subjected to similar enforcement measures as the other mentioned types of infringing content, measures which encounter similar challenges. Moreover, there are certain crucial provisions of the EU law which apply to all four types of infringing content – for example, the "safe harbours" of the E-Commerce Directive,

[2] Described in section 3.1.2.2 of chapter two.
[3] Described and explored further in section 3.2 of chapter four.
[4] See chapter four, section 3.2.1.
[5] Though it should be noted that privacy and reputation can be seen as protected by a single human right, the right to privacy – see section 2.2 of chapter four.

limiting the liability of various intermediaries.[6] In order to demonstrate how defamatory content might come to existence, chapter one relies on the law of England and Wales, which has oftentimes dealt with the legal issues surrounding the removal of online access to defamatory content. Additionally, cases from further jurisdictions are used sparingly in order to demonstrate a wide selection of scenarios leading to the spread of infringing content.

In terms of structure, this chapter is made of four primary sections, each of them focused on a different category of infringing content. Furthermore, each of those sections is divided into two parts; the first, describing the legal framework governing the recognition process of the given category of infringing content, and the second, presenting an overview of the principal factual scenarios which are likely to lead to such recognition.

2. Copyright-infringing content.

2.1. European Union's legal framework governing the identification of copyright-infringing content.

Whether we look towards article 17(2) of the Charter of Fundamental Rights of the EU (which states that "intellectual property should be protected"[7]), or more specifically, to recital 9 of the Information Society Directive (which states that "any harmonisation of copyright and related rights must take as a basis a high level of protection, since such rights are crucial to intellectual creation"[8]), it is clear that protection of copyright is a well-established concept within the EU legal framework. While there is a variety of harmonised rights

[6] See chapter two, section 3.3.
[7] The Charter of Fundamental Rights of the European Union (2000/C 364/01), art. 17(2).
[8] 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, rec. 9.

on which EU copyright owners can rely on, two of them are of particular significance in situations involving the exchange of digital content online; the right of reproduction and the right of communication to the public. As such, they deserve to be introduced in the following paragraphs.

2.1.1. The right of reproduction.

The right of reproduction is the eldest and most traditional form of copyright protection. On the international level, it is set out in art. 9(1) of the Berne Convention, which states that "authors of literary and artistic works protected by this Convention shall have the exclusive right of authorizing the reproduction of these works, in any manner or form".[9] Later on, this provision has been reaffirmed both in the TRIPS Agreement, art. 9(1) of which states that "Members shall comply with Articles 1 through 21 of the Berne Convention (1971) and the Appendix thereto. (…)",[10] and in the WIPO Copyright Treaty (WCT) 1996, art. 1(4) of which states that the "Contracting Parties shall comply with Articles 1 to 21 and the Appendix of the Berne Convention".[11] In case of the latter treaty, it is worth mentioning its inclusion of an agreed statement concerning article 1(4), which underlines that "the reproduction right, as set out in Article 9 of the Berne Convention, and the exceptions permitted thereunder, fully apply in the digital environment, in particular to the use of works in digital form".[12]

This internationally embraced form of the right of reproduction truly found its way into the European Union's law with the appearance of the Information Society Directive, which (among others) implemented the provisions of the WCT 1996 into the EU law.[13] Article 2 of this directive states that:

[9] Berne Convention 1886, art. 9(1).
[10] The Agreement on Trade-Related Aspects of Intellectual Property Rights 1994, art. 9(1).
[11] WIPO Copyright Treaty 1996, art. 1(4).
[12] TRIPS, supra fn. 11, agreed statement concerning Article 1(4), at fn. 1.
[13] Information Society Directive, supra fn. 8, rec. 15.

- "Member States shall provide for the exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part:
    - (a) for authors, of their works;
    - (b) for performers, of fixations of their performances;
    - (c) for phonogram[14] producers, of their phonograms;
    - (d) for the producers of the first fixations of films, in respect of the original and copies of their films;
    - (e) for broadcasting organisations, of fixations of their broadcasts, whether those broadcasts are transmitted by wire or over the air, including by cable or satellite".[15]

It should be noted here that, as Walter and Von Lewinski pointed out,[16] while the Computer Programs Directive[17] and the Database Directive[18] harmonised the right of reproduction for software and databases respectively, art. 2 of the Infosoc Directive covered all categories of copyrighted works; software and databases included. For this reason, it is going to serve in this subchapter as a point of reference in factual scenarios focused on the digital content which infringes copyright by means of reproduction.

2.1.2. The right of communication to the public.

Similarly to the right of reproduction, the origins of the EU-harmonised right of communication to the public can be seen as lying primarily within two articles of the Berne Convention. Firstly, art. 11 gives the authors of "dramatic, dramatico-musical and musical works"[19] the exclusive right of

[14] A term denoting a sound recording.
[15] CFREU, supra fn. 8, art. 2.
[16] Walter M and Von Lewinski S, *European Copyright Law: A Commentary* (OUP 2010), at 964.
[17] Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, art. 4.
[18] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, art. 5.
[19] Berne Convention, supra fn. 9, art. 11(1).

authorizing "any communication to the public of the performance of their works".[20] Secondly, art. 11bis gives the authors of "literary and artistic works" the exclusive right of authorising:

- "(i) the broadcasting of their works or the communication thereof to the public by any other means of wireless diffusion of signs, sounds or images;
- (ii) any communication to the public by wire or by rebroadcasting of the broadcast of the work, when this communication is made by an organization other than the original one;
- (iii) the public communication by loudspeaker or any other analogous instrument transmitting, by signs, sounds or images, the broadcast of the work".[21]

Additionally, specialised variants of the right of communication to the public can also be found in art. 11ter (focused on recitations of literary works), as well as in articles 14 and 14bis (focused respectively on cinematographic adaptations of literary and artistic works and cinematographic works in general).

The described provisions of the Berne Convention were reiterated and updated in the two World Intellectual Property Organisation Treaties of 1996, the WCT 1996 and the WIPO Performances and Phonograms Treaty (WPPT) 1996. First of all, art. 8 of the WCT (which, according to Walter and Lewinski, filled the gaps in the Berne Convention's take on the right of communication to the public[22]) states that:

- "Without prejudice to the provisions of Articles 11(1)(ii), 11*bis*(1)(i) and (ii), 11*ter*(1)(ii), 14(1)(ii) and 14*bis*(1) of the Berne

[20] Berne Convention, supra fn. 9, art. 11(1).
[21] Berne Convention, supra fn. 9, art. 11bis(1).
[22] Walter and Lewinski, supra fn. 16, at 975.

Convention, authors of literary and artistic works shall enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them".[23]

Secondly, art. 10 of the WPPT concentrates on the performers and provides that they:

- "(…) shall enjoy the exclusive right of authorizing the making available to the public of their performances fixed in phonograms, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them".[24]

Finally, art. 14 of the WPPT focuses on the producers of phonograms, and grants them:

- "(…) the exclusive right of authorizing the making available to the public of their phonograms, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them".[25]

The influence of the earlier mentioned articles of the WIPO treaties can be seen in the wording of article 3 of the Information Society Directive, which is the principal regulatory provision harmonising the right of communication to the public within the EU. Firstly, it grants authors the right to:

[23] WCT, supra fn. 11, art. 8.
[24] WIPO Performances and Phonograms Treaty 1996, art. 10.
[25] WPPT, supra fn. 24, art. 14.

- "authorise or prohibit any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them".[26]

Secondly, in section 3(2), art. 3 addresses four further categories of entities, stating that:

- "Member States shall provide for the exclusive right to authorise or prohibit the making available to the public, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them:
    - (a) for performers, of fixations of their performances;
    - (b) for phonogram producers, of their phonograms;
    - (c) for the producers of the first fixations of films, of the original and copies of their films;
    - (d) for broadcasting organisations, of fixations of their broadcasts, whether these broadcasts are transmitted by wire or over the air, including by cable or satellite".[27]

Furthermore, those provisions are supported by art. 8 of the Rental and Lending Directive.[28] First of all, it gives the performers:

- "the exclusive right to authorise or prohibit the broadcasting by wireless means and the communication to the public of their performances, except where the performance is itself already a broadcast performance or is made from a fixation".[29]

[26] Information Society Directive, supra fn. 8, art. 3(2).
[27] Information Society Directive, supra fn. 8, art. 3.
[28] Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property.
[29] Rental and Lending Directive, supra fn. 28, art. 8(1).

Additionally, it bestows upon the broadcasting organisations:

- "the exclusive right to authorise or prohibit the rebroadcasting of their broadcasts by wireless means, as well as the communication to the public of their broadcasts if such communication is made in places accessible to the public against payment of an entrance fee".[30]

2.2. Factual scenarios leading to the transfer of copyright-infringing content.

This subsection aims to present an accurate overview of the main categories of factual scenarios recognised (or likely to be recognised) as infringing the harmonised rights described in the preceding paragraphs.

Amongst the four legitimate interests covered in this thesis, copyright truly "shines" when it comes to the variety of information technologies through which this legitimate interest can be infringed by means of the exchange of digital content. Hence, this subsection is divided on four segments, each of them focused on a specific category of online resources used for the discussed mode of infringement. The first three segments (focused respectively on cyberlockers, streaming websites and P2P networks) are related to the phenomenon of copyright-infringing filesharing, with the fourth segment focused on image search and news-aggregation services, and their role in facilitating access to publicly available, legitimately uploaded content protected by copyright.

2.2.1. Cyberlockers.

[30] Rental and Lending Directive, supra fn. 28, art. 8(3).

One-click hosting websites, also known as cyberlockers, have oftentimes been indicated as one of the primary sources of copyright-infringing content in cyberspace.[31] As Garstka wrote in 2012, the simplicity of this category of online resources (upload a file, get a link to the file, share the link), conjoined with the reward policy employed by many operators of cyberlockers (where uploaders get rewarded if their files are popular among the downloaders) turned many of these websites into online pirate's treasure chests[32] – after all, there are few categories of digital content more desired by the online community than free copyrighted music, films or games. Examples of popular one-click hosting websites include Rapidshare[33], Mediafire[34] or Megaupload[35]- with the first and last one having been subjected to major legal proceedings.

Additionally, responding to the demand for indexing services attached to one-click hosting websites, search engines (such as Filestube[36] or FileDiva[37]) emerged, scouring the Net for cyberlocker links to specific files demanded by their users. Their task is facilitated by the existence of online forums, wholly or partially dedicated to hosting and indexing those links (a good example here would be Ledix.com[38]). As one might guess, a fair amount of links shared through such portals leads to copyright-infringing content.[39]

Since this thesis is focused on the European Union, it is necessary to place the activities described above within the context of articles 2 and 3 of the Information Society Directive. Let us start with the former, establishing the

[31] *Technical report: An Estimate of Infringing Use of the Internet* (2011) Envisional, at. 2, accessible at: http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf. (NOTE: All websites cited in this work were last accessed on 15.03.2016.)
[32] Garstka K, 'The Amended Digital Economy Act 2010 as an Unsuccessful Attempt to Solve the Stand Alone Complex of Online Piracy' (2012) IIC 43(2), 158, at 162.
[33] No longer accessible.
[34] Accessible at: http://www.mediafire.com/.
[35] No longer accessible.
[36] No longer accessible.
[37] Accessible at http://filediva.com.
[38] No longer accessible.
[39] For example, the operator of Ledix was found guilty of criminal copyright infringement in March 2013, see http://the1709blog.blogspot.co.uk/2013/03/linking-site-operator-convicted-by.html.

harmonised right of reproduction. In case of cyberlockers, it is submitted that this right is liable to be infringed in at least two stages of the process; the copyrighted work is "reproduced" (within the meaning of art. 2) whenever a user uploads it onto a cyberlocker (thus, creating its copy on the website's server), as well as whenever another Internet user downloads it (reproducing it on his computer).

As for the right of communication to the public, set out in art. 3 of the InfoSoc Directive, it seems likely to be infringed in the discussed setting on at least two occasions. Firstly, whenever a user uploads a copyrighted file (onto a cyberlocker) in such a way that it is available to anyone with the right link;[40] and secondly, perhaps much more significantly, whenever the said link is shared on, for example, online forums and is consequently located by various indexing services. It can be argued that in both instances, the file is "made available to the public", oftentimes by both wire *and* wireless means, and at a time individually chosen by the members of the public; and that therefore, both of the discussed instances meet the criteria set out in the earlier mentioned Directive.[41]

However, the conclusion reached in the previous paragraph has to be placed in the light of the CJEU decision in the *Svensson* case (2014),[42] which stated that art. 3 "must be interpreted as meaning that the provision on a website of clickable links to works freely available on another website does not constitute an 'act of communication to the public'".[43] This is due to the so-called 'new public' criteria, according to which communication to the public persists only where the act made the work available to a new group of recipients. Works which are freely available were regarded by the Court as aimed at the whole cyberspace – "given that access to the works on that site was not subject to

[40] It should be remembered that it is oftentimes possible to use a cyberlocker in the "private mode", where only the uploader may access his content – in this case, we cannot really speak of communication to the public.
[41] Information Society Directive, supra fn. 8, art. 3.
[42] NOTE: Throughout this thesis, case names cited in the body of the text will be accompanied by the year the judgement was published, given in „()" brackets. This is done for the informative purpose and does not indicate the instance of the court which gave the decision.
[43] Case C-466/12 *Svensson v Retriever Sverige AB* [2014], at [32]

any restrictive measures, all Internet users could therefore have free access to them".[44] However, this decision dealt with linking to content which – in contrast to the content this thesis focuses upon - is legitimately uploaded. Hence, the *Svensson* ruling could be seen as neutral to the presented analysis of art. 3 of the InfoSoc Directive, neither in this, nor other sections of this chapter if it was not for the *Bestwater* case (2014).[45]

This decision dealt with copyright-infringing content *per se*, and the Court's judgement confirmed and extended the principle established in *Svensson*, stating that embedding/framing a video on one's website might constitute communication to the public, if that public is a new one.[46] However, given that the Court did not draw a distinction between the content uploaded by the copyrightholder/his proxy and content uploaded without the copyrightholder's consent, it seems that *Svensson* applies to the provision of links to infringing files on cyberlockers. Such an action could theoretically be seen as communication to the public, but due to the interpretation of the 'new public' criteria, this is unlikely to ever occur. In any case, the path of infringement's recognition based on the right of reproduction continues to provide a basis for the inclusion of cyberlockers in this chapter.[47] [48]

Complementary evidence of the copyright-infringing use of cyberlockers can be inferred from a number of legal cases brought against the operators of such services. In order to demonstrate the basis for such an assumption, I shall focus this subsection on proceedings brought against three one-click hosting websites; Rapidshare, Uploaded.to, as well as Megaupload.

The first of the three examples is the Dusseldorf Higher Regional Court's

[44] *Svensson*, supra fn. 43, at [26]
[45] Case C-348/13 *BestWater International GmbH v Michael Mebes and Stefan Potsch* [2014]
[46] *BestWater*, supra fn. 45, at [19].
[47] For further discussion of hyperlinking as an infringing activity, see the Supreme Court of Canada's decision in the defamation case of *Crookes v Newton* [2011] SCC 47.
[48] Given the age of the Web, it is somewhat surprising that the issue of hyperlinking to allegedly copyright-infringing content has only recently come up for consideration by the CJEU, see the (at the time of writing) upcoming decision in Case C-160/15 *GS Media BV v Sanoma Media Netherlands BV and Others*,

decision in the case of *Atari v Rapidshare* (2010).[49] The operators of this cyberlocker have been sued by the videogames company Atari, who claimed that multiple copies of their game called *Alone in the Dark* were shared illegally through the defendant's hosting service. Among others, the said company wanted to obtain a court order forcing Rapidshare to filter the content hosted on their servers and delete files containing certain keywords (such as the name of the game in question).

While the order in question was not granted,[50] such injunctions are given thorough attention in chapter two, as they are a representation of one of the enforcement strategies this thesis is focused upon.[51] For now, the noteworthy aspect of the discussed case is that the operators of Rapidshare did not try to deny the existence of the infringing activity in question. Moreover, the judge himself remarked that it is indisputable that filesharing activities occurring on the defendant's platform infringed Atari's copyright within the meaning of the German copyright law[52]- which, in accordance with the Directives mentioned above, grants the copyright owners an exclusive right of reproduction[53] and right of communication to the public.[54]

Uploaded.to appeared in 2006, and gained a considerable popularity among the filesharing community due to its (then) favourable upload limits (up to 250 megabytes per file) and a generous reward scheme – for each file which was downloaded at least a thousand times, its uploader was paid four euros.[55] Since, as one could expect, a considerable amount of files shared through this service was copyright-infringing, website operators received complaints from the rightholders as early as 2007, and later on, they were charged with criminal copyright infringement in 2013.

---

[49] OLG Düsseldorf, 21 December 2010, I-20 U 59/10.
[50] See chapter two, section 3.1.2.2.
[51] See chapter two, section 3.1.2.2.
[52] *Atari v* Rapidshare, supra fn. 49, at [20].
[53] Gesetz über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz) (geändert am 17. Dezember 2008) [Law on Copyright and Related Rights (as amended December 17, 2008)], art. 16.
[54] Law on Copyright and Related Rights, supra fn. 53, arts. 21 and 22.
[55] See http://torrentfreak.com/former-uploaded-to-admin-fined-188000-for-copyright-infringement-130227/.

Once more, it is quite telling that the existence of infringing activity on the cyberlocker was not challenged before the District Court of Munich, which heard the earlier mentioned case in 2013.[56] Building upon this preliminary finding, it found the operator of Uploaded.to guilty of commercial copyright infringement and sentenced him to pay a total fine of 144,000 euros, divided on 360 day fines of 400 euros each.[57]

Finally, the last case to be mentioned here is the criminal trial of the operators of Megaupload, or (as the indictment document prefers to call them) the "Mega Conspiracy".[58] Before it was taken down in January 2012, Megaupload was probably the largest and most influential cyberlocker in cyberspace, easily making it (at its height) to the Top 60 most visited websites in the world.[59] As one could (once again) imagine, a considerable amount of this website's traffic consisted of copyright-infringing filesharing; consequently, on the 19th of January 2012, the owners and operators of this cyberlocker were arrested on multiple charges (starting with criminal copyright infringement)[60] and their servers were seized by the federal government of the United States.

At the time of writing, the case still remains in the state of being processed, mainly because of due process and extradition matters. Regardless of its outcome, it is once again worth to note that Megaupload's lawyer, Ira Rothken, did not try to dismiss the existence of widespread copyright-infringing filesharing which occurred on his client's cyberlocker.[61]

Concluding; without dismissing the legal use of one-click hosting websites, the three cases described above show that there can be little doubt that cyberlockers in general became used as networks for copyright-infringing

[56] The *Uploaded.to* case (2012) AG Munich, Az.1111 Cs 404 Js 44538/07.
[57] For more on criminal copyright infringement, see chapter two, sections 2.2 and 3.2.
[58] Indictment document accessible at: http://www.scribd.com/doc/78786408/Mega-Indictment, at [1].
[59] See http://www.alexa.com/siteinfo/megaupload.com.
[60] Megaupload indictment, supra fn. 58.
[61] See the interview at http://www.washingtonpost.com/business/technology/megaupload-lawyer-qanda-on-doj-criminal-case/2012/01/20/gIQA3HJhDQ_story.html.

filesharing. While some of them, such as Megaupload, met their fate as a result of this state of affairs, many cyberlockers – 4shared,[62] Mediafire, Rapidgator,[63] Turbobit,[64] to mention a few - continue to operate, and accordingly, the infringing activity taking place on platforms such as those must be approached in this thesis.

2.2.2. Web 2.0[65] streaming websites.

Web 2.0 streaming websites form the second category of online resources which are facilitating the creation and spread of copyright-infringing content in cyberspace, by giving rise to factual scenarios which are liable to infringe the harmonised rights of reproduction and communication to the public. In a way, they function similarly to cyberlockers, in that they allow their users to upload files and share them with others by means of an associated link to the file. However, the act of sharing occurs here not through the act of downloading, but by playing back the uploaded content directly through the service provider's website. Consequently, two principal categories of digital content have come to be shared through this platform, this being audio and audiovisual files.[66]

Popular examples of streaming websites include portals such as Grooveshark,[67] (audio files) Youtube,[68] Dailymotion,[69] Putlocker[70] or Megavideo[71] (audio-visual files). Similarly to cyberlockers, such services are

[62] Accessible at http://4shared.com
[63] Accessible at: http://rapidgator.net/.
[64] Accessible at: http://turbobit.net/.
[65] The term web 2.0 describes a stage of the Internet's development, characterised by the arrival and increasing popularity of online services allowing for the exchange of user-generated content, that is content created and/or uploaded by the services' users, as opposed to the services' operators.
[66] There are some notable, innovative exceptions to this statement, such as the Onlive service (accessible at: http://www.onlive.com/) which was based around the interactive streaming of PC games, but so far, there are no signs of infringing activity occurring in this sector.
[67] Accessible at: http://groovesharks.org/.
[68] Accessible at: https://www.youtube.com/.
[69] Accessible at: http://www.dailymotion.com/.
[70] Accessible at: http://www.putlocker.is/.
[71] No longer accessible.

supported by indexing websites, such as 1channel,[72] Movie2k[73] (for movies and TV series), or Anilinkz[74] (for Japanese anime), as well as by online forums, such as ItalianShare,[75] hosting links to content uploaded on streaming websites.

As it was the case with one-click hosting websites, this category of online resources also became used for widespread illegal filesharing of copyrighted content, a development most likely to contravene articles 2 and 3 of the InfoSoc Directive in a manner similar to that described in section 2.2.1 of this thesis. That being said, streaming websites might differ here from cyberlockers in two ways. Firstly, whenever a user accesses an infringing file on the streaming website, it is reproduced on his computer in two primary ways, accurately indicated by Borghi as buffering (which "is an act of temporary storage in the temporary memory, and it is inherent to the streaming process") and caching (which can be seen as "temporary storage in the permanent memory, (…) ancillary or subsidiary to streaming").[76] The cited writer provides a robust analysis of the connection between those acts and the right of reproduction,[77] and it is worth to refer to the said interplay in this section. Normally, the user of a streaming website does not reproduce the whole, independent, "shareable" file. However, art. 2 of the InfoSoc Directive explicitly incorporates "temporary or permanent reproduction by any means and in any form",[78] what indicates that it could cover the described act as well. Then again, art. 5(1)(a) of the same instrument provides that "temporary acts of reproduction referred to in Article 2, which are transient or incidental [and] an integral and essential part of a technological process", as well as only aimed at facilitating a lawful transmission between third parties, by an intermediary, are to be exempted from the scope of the right of reproduction.[79] This could be seen as applying to buffering, the essential component of

[72] Accessible at: http://www.1channel.biz/.
[73] Accessible at: http://www.movie2k.io/.
[74] Accessible at: http://anilinkz.tv/.
[75] No longer accessible.
[76] Borghi M, 'Chasing copyright infringement in the streaming landscape' (2011) IIC 42(3), at 328.
[77] Borghi, supra fn. 76, section II.
[78] Information Society Directive, supra fn. 8, art. 2.
[79] Information Society Directive, supra fn. 8, art. 5(1)(a).

streaming; though the lawfulness of the transmission could be questioned on the basis of the right of communication to the public. Additionally, there is an argument that streaming-related acts of reproduction might fall short of the intellectual creation test laid out in the CJEU case of *Infopaq*.[80]

Secondly, in contrast to cyberlockers, major streaming websites often field their own search facilities – consequently, in the light of art. 3 of the InfoSoc Directive, the mere act of uploading an infringing file might make for an even stronger case of unauthorised communication to the public.

As this thesis is focused on the enforcement mechanisms and the point in which it is clear that content is infringing, this section is going to stop here, by resting on the position that copyright-infringing streaming has the capability to infringe both arts. 2 and 3 of the InfoSoc Directive. The latter one should arguably see more use in this context, as it is plausible to agree with Borghi that the clearly interpreted right of communication to the public is a much more suitable response to such streaming than the right of reproduction, which "face to the evolving technologies (…) is the more and more ill suited to be used as the main detector of infringement"[81] – as the complex artificiality of its application, discussed above, shows.

It is also worth to add that although copyright-infringing activities came to occur on both video and music streaming services, it is the former category which attracted the lion's share of copyright holders' attention, probably for a good reason – while a music file can be uploaded onto a video streaming website, the same cannot be said about uploading an audiovisual file onto a music streaming portal.

In order to provide examples for this section of the subchapter, it seems appropriate to look at the largest and most popular video streaming website,

[80] Covered in section 2.2.4.2 of the current chapter.
[81] Borghi, supra fn. 76, at 343.

YouTube.[82] Aside from a huge amount of User Generated Content (UGC) uploaded by users to the site, there are uploads of works for which the uploader does not appear to be the copyright owner; although the copyright owner may have allowed the upload via YouTube's Content ID system mentioned in the Introduction above.

It is no surprise that the operators of Youtube have visited many courtrooms, in various parts of the world. This subsection is going to mention three such legal cases, sharing a common trait; none of them included a significant challenge to the notion that this streaming website was used for sharing the copyrighted content in question. In the first case, *Telecinco v Youtube* (2010),[83] the streaming website was (unsuccessfully) sued for facilitating copyright infringement of audiovisual files belonging to a Spanish television channel.[84] Next, in the case of *TF1 v Youtube LLC* (2012),[85] also based on the spread of content belonging to a television channel, the judge noted that the main point of contention in the case at hand is defining the status of Youtube's operators and whether they can be liable for the copyright infringements as publishers[86] – not whether the infringements occurred. Finally, in the American case of *Viacom International v Youtube* (2010),[87] the claimant global media organisation sued Youtube (also unsuccessfully) for facilitating the repeated infringements of over 150,000 works belonging to them and their joint claimants.[88]

Now, if we turn to the earlier mentioned indexing services and forums used for facilitating access to the files hosted on the streaming websites, they became used for copyright-infringing purposes in the same way as their cyberlockers-

[82] At the time of writing, the 3rd most popular website in the world – see http://www.alexa.com/ siteinfo/youtube.com.
[83] 289/2010, at Commercial Court no.7 (Madrid).
[84] For further coverage of this decision, see section 3.1.2.2 of chapter two.
[85] Court of First Instance Paris, judgment delivered on the 29th of May 2012.
[86] *TF1 v Youtube LLC*, supra fn. 85, at 24.
[87] 07 Civ. 2103 (LLS).
[88] See Viacom's complaint, accessible at: http://online.wsj.com/public/resources/documents/ ViacomYouTubeComplaint3-12-07.pdf, at [3]. The US courts held that YouTube's procedures regarding responding to notices of infringement fell within the Digital Millenium Copyright Act's framework and the dispute settled.

focused counterparts.[89] Accordingly, they have also gained the attention of copyrightholders and their lawyers. An example of a resulting legal action is provided by the British case of *R. v Rock and Overton* (2010),[90] where the operator of a website known as TV Links (which hosted links to streaming websites, such as Megavideo) was charged with criminal copyright infringement and conspiracy to defraud. In the end, he was protected from liability by one of the E-Commerce Directive's safe harbours[91] (covered in detail in chapter two[92]); for now, this indicates that liability-inducing activity was indeed occurring on the contested website. Other cases involving similar websites are, for example, the Italian trial of an individual known as Tex Willer (operator of ItalianShare),[93] and the trial of the operator of Surf The Channel (a video search engine),[94] which took place in England. In both of those cases, the operators were held liable for the infringements occurring on their services.

There is an additional dimension to the infringement of copyright on various web streaming services, and it should be mentioned in this subsection. The initial presumption is that whenever a user is receiving streamed content, he does not come to possess the file in question like he would upon downloading it from a cyberlocker. However, with the development of specific websites (such as vid2mp3.com[95]) and web browser add-ons (such as the Download Helper[96]), users became able to download the files from streaming websites as well.[97] What this effectively means is that the copyright-protected content uploaded to streaming portals might travel a much farther route than one could anticipate, infringing the rights of reproduction and of communication to the

[89] It should be added that some of those websites can be facilitating access to content hosted on both cyberlockers and streaming websites.
[90] T20087573 (at Gloucester Crown Court).
[91] 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, art. 12.
[92] See chapter two, section 3.3.1.
[93] See https://torrentfreak.com/former-file-sharing-site-admin-fined-6-4-million-euros-130219/.
[94] See http://www.guardian.co.uk/technology/2012/aug/14/anton-vickerman-surfthechannel-sentenced.
[95] See http://www.vidtomp3.com/.
[96] See https://addons.mozilla.org/en-US/firefox/addon/video-downloadhelper/.
[97] It is worth adding that the existence of such services was recognised by, among others, the judge in the *Telecinco* case, supra fn. 83, at 5.

public to an even more extensive degree. A good example here are the music artists who decided to upload their works on Youtube via official Youtube channels (such as those run by Vevo[98]) – while they might be under the impression that users who want to listen to their music will have to buy it through a legitimate channel in order to be able to, for example, upload it to their mobile devices, the development of the earlier mentioned services might be, to an extent, dismantling this assumption.

While it was mentioned in the beginning of this subsection that music streaming websites attract arguably less copyright-infringing activity than their video streaming counterparts, there are some notable examples of legal cases involving portals belonging to the former category. In the US case of *UMG Recordings v Escape Media Group* (2012)[99], the operators of a music streaming website known as Grooveshark (which operates much in the same manner as Youtube, it hosts user-uploaded music tracks) were sued by UMG, but ended up being protected by the Digital Millennium Copyright Act 1998 (hereafter referred to as the DMCA 1998)'s safe harbour.[100] And moving back to the EU, in 2007, the operators of Myspace (one of the most well-known music streaming websites) were found by the Paris High Court of the First Instance to be liable for the copyright infringements committed by their users.[101]

Finally, it is worth mentioning two more aspects of copyright infringement occurring by means of digital content hosted on the streaming websites. Firstly, on top of streaming standard, stand-alone files, some websites allow for the streaming of live, broadcasted content; this form of transmission can also give rise to liability for copyright infringement, as it happened in the English case of *ITV Broadcasting v TV Catchup* (2011).[102] Secondly, as the Court of Justice of the European Union (hereafter referred to as the CJEU)

[98] For example, see https://www.youtube.com/user/DidoVEVO.
[99] Inc. 37 Misc.3d 208, 948 N.Y.S.2d 881 N.Y.Sup.
[100] *UMG Recordings v Escape Media Group*, supra fn. 99, at 27. For further coverage of the intermediary liability safe harbours, see section 3.3 in chapter two.
[101] The *Myspace* case (2007), Tribunal of Grand Instance Paris, judgment delivered on the 13th of July 2007.
[102] [2011] EWHC 1874 (Pat).

case of *Netlog* (2012)[103] demonstrates, it might happen that a social media website adopts the infrastructure of a streaming website, what might also complicate any enforcement mechanisms undertaken against the infringements occurring on such a hybrid website.[104]

2.2.3. P2P networks.

The third category of online resources covered in this subsection are the P2P networks. This method of exchanging files in cyberspace is fundamentally different from one-click hosting and streaming websites – here, the files are (in principle) exchanged between the users' computers, instead of being uploaded to an intermediary website. On the other hand, similarly to the online resources covered in the previous two subsections, P2P networks have also become used for widespread copyright-infringing filesharing, leading to cases such as *Scarlet Extended v SABAM* (2011),[105] which dealt with the liability of Internet Service Providers[106] (hereafter referred to as ISPs) for P2P copyright infringement occurring via their services. Looking back to the earlier mentioned Envisional report, it estimates that in terms of traffic, P2P networks were responsible for 72 % of all copyright infringing activities on the Internet in 2011.[107] It is therefore crucial to identify and understand the main types of P2P networks, which are used in the manner which made for this rather impressive number.

2.2.3.1. BitTorrent.

In terms of traffic, the BitTorrent platform is likely to still be the most popular method of exchanging files on the Internet.[108] To summarise the way it works (in the most common pattern); first of all, the user wishing to obtain a file

---

[103] Case C-360/10 *Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) v Netlog NV* [2012].
[104] See chapter two, section 3.3.1.2.
[105] Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011].
[106] Intermediaries primarily providing the users with the basic Internet connection.
[107] Envisional, supra fn. 31, at 2.
[108] Envisional, supra fn. 31, at 2.

from this platform must download a piece of software known as the BitTorrent client. Then, he has to locate and download a small .torrent file (commonly referred to as a torrent), which is going to act as a "beacon" on the BitTorrent network. Subsequently, with the help of a torrent tracker (a server directing the BitTorrent traffic), he is able to locate computers on the network which are "seeding" the file which he wants to obtain, (that is making available the "saturated" version of its corresponding torrent file) and start downloading the parts of this file from all those users. Once his .torrent file "fills up", he can access the content it was directing to. It must be added that even while the user is still downloading the parts of his desired file, he is (in the most common scenario) allowing others to download from him the parts of the file which he has already obtained – moreover, the user's download speed is often increased depending on how many files did he seed/make available, thus providing an incentive to share.

The described architecture of the BitTorrent protocol makes it extraordinarily efficient in transferring large files (such as movies or video games). And it is perhaps due to this efficiency, and the distinct sense of community (which might be resulting from the give and take-based exchange of content), that the BitTorrent protocol has become widely recognised as a platform used for copyright-infringing filesharing. To demonstrate a specific example of such activity; according to an inquiry conducted by Torrentfreak, in 2012, a single episode of the popular TV series *Game of Thrones* was being downloaded via BitTorrent 4,280,000 times.[109]

It is submitted that infringing activities occurring through the use of the BitTorrent platform are very much likely to lie in contravention of both article 2 and 3 of the InfoSoc Directive. The right of reproduction seems to be infringed here on at least two occasions. Firstly, it can be argued that reproduction occurs whenever users are downloading parts of the seeded (copyrighted) file, since art. 3 covers reproduction "in whole or in part" and

[109] See http://torrentfreak.com/game-of-thrones-pirates-break-bittorrent-swarm-record-130401/.

"by any means and in any form".[110] Secondly, and perhaps more importantly, reproduction occurs whenever the user completes the download, obtaining a full, accessible copy of the desired file. As for the right of communication to the public, it is plausible to state that whenever someone seeds a copyrighted file on a torrent network, he is making it available to the public; moreover, as it was mentioned in the previous paragraphs, those who download the said file, are oftentimes simultaneously making the already downloaded parts of it available to others.

In terms of case law, recent years saw an abundance of cases indicating the existence of copyright-infringing activity on the BitTorrent platform. First of all, in 2009, the District Court of Stockholm found the operators of The Pirate Bay (probably the most well-known BitTorrent indexing website, which also provided torrent trackers) criminally liable for facilitating the copyright-infringing exchange of files on the BitTorrent network,[111] a judgment which was later upheld on by the Swedish Court of Appeal.[112] In the UK, the case of *R. v Alan Ellis* (2010)[113] saw the operator of Oink's Pink Palace (which was a BitTorrent-orientated music sharing website running a torrent tracker) charged with conspiracy to defraud, and acquitted of it by the jury – nevertheless, the existence of infringing activities on the website was undisputed. And for the last example, this paragraph can refer to a Dutch case centred on the SumoTorrents website,[114] which was (and at the time of writing, still is[115]) indexing torrent files. In this particular legal action, the presence of copyright-infringing activities was confirmed by the court, but due to specific factual circumstances,[116] it was the SumoTorrents' ex-hosting provider who became liable for damages.

Furthermore, the infringing activity occurring on torrent websites made them a

[110] Information Society Directive, supra fn. 8, art. 3.
[111] Case B-13301-06, District Court of Stockholm, judgment delivered on the 17th of April 2009.
[112] See http://www.guardian.co.uk/technology/2010/nov/26/pirate-bay-founders-appeal.
[113] T20087573 (at Middlesborough Crown Court).
[114] See http://www.bbc.co.uk/news/technology-20080628.
[115] See http://sumotorrents.eu.
[116] BBC, supra fn. 114.

prime target for blocking injunctions in many countries. Starting with the court order in the UK case of *Dramatico Entertainment v British Sky Broadcasting (No. 2)*(2012)[117] (aimed at The Pirate Bay, which is most probably the European record holder in this category), through a series of Italian decisions, ordering the ISPs of that country to block access to torrent websites such as TorrentReactor and Torrents.net,[118] to another case from the UK, *EMI Records v British Sky Broadcasting* (2013),[119] where three further torrent websites (KickassTorrents, H33t and Fenopy) became the subject of a blocking injunction as well.

2.2.3.2. Usenet.

The second P2P network covered in this section is the global distributed discussion system known as Usenet. It is accessed through a piece of software called a newsreader client, and operates through an array of so-called newsgroups. Initially, the newsgroups were purely text based; this changed with the development of alt.binaries newsgroups, allowing for the exchange of files such as films, music, or software. Consequently, Usenet's traffic rose considerably –while in 2000, the daily transfer to all newsgroups equalled to 0.282 TB, in September 2010, it rose to 8 TB per day.[120]

The development of infrastructure allowing Usenet users to share binary files turned this discussion system into a yet another platform for copyright-infringing filesharing contravening the InfoSoc Directive's provisions. It seems fair to say that "reproduction" (within the meaning of art. 2) occurs here on at least three occasions; whenever a user uploads the copyrighted file onto the Usenet news servers, whenever the file is transferred from one news server to another, and whenever another user downloads the said file from a newsgroup onto his own computer. Looking from the art. 3 angle, it is plausible to indicate that the copyrighted file is "made available to the public"

[117] [2012] EWHC 1152 (Ch).
[118] See http://torrentfreak.com/italian-court-orders-nationwide-block-of-torrentreactor-and-torrents-net-121204/.
[119] [2013] EWHC 379 (Ch).
[120] See http://www.newsdemon.com/average_feed_size.php.

whenever a user uploads the file to a Usenet newsgroup.

In terms of the infringing traffic, the Envisional report states that Usenet comes nowhere near the BitTorrent platform, the former claiming mere 3,6 % of the global infringing transfer in 2011.[121] Nevertheless, the operators of Usenet-related websites also became subjected to legal actions prompted by the copyrightholders. In the UK case of *Twentieth Century Fox Film Corp v Newzbin* (2010),[122] the operators of a Usenet indexing website (which was found to have been used for illegal exchange of copyrighted movies) were found liable for the infringing activities of their users. Another Usenet indexing website, NZBMatrix, voluntarily shut down, citing an overloading amount of received takedown notices as the reason.[123] Finally, Usenet-Crawler (the third website of the same kind) was taken down as a result of a letter sent by the BREIN anti-piracy outfit to Usenet-Crawler's hosting provider.[124]

2.2.3.3. Other P2P networks.

Apart from the BitTorrent platform and Usenet, there are many other P2P file exchange networks out there, many of which became used for copyright-infringing activities, leading to corresponding legal actions. The first examples here are provided by the classic US cases of *Napster* (2001)[125] and *Grokster* (2005)[126] where liability for users' copyright infringement was placed (respectively) on operators and marketers of two different P2P filesharing programs; as a result of those cases, both services were effectively forced to close down.

While Napster returned later on as a licensed, "legal" service, it is worth to outline its initial form, the infringing use of which led to the mentioned legal case. Firstly, each Napster user had to download the client software and choose the files he would like to add to the program's dedicated music library.

[121] Envisional, supra fn. 31, at 2.
[122] [2010] EWHC 608 (Ch).
[123] See http://torrentfreak.com/nzbmatrix-shuts-down-citing-piracy-troubles-121209/.
[124] See https://torrentfreak.com/anti-piracy-group-takes-usenet-crawler-offline-130405/.
[125] *A&M Records, Inc. v Napster, Inc.* (2001) 239F.3d 1004, 9th Circuit.
[126] *MGM Studios, Inc. v Grokster, Ltd.* (2005) 545 U.S. 913.

Upon connecting to the Napster network, each individual user's library was communicated to the central indexing server. Consequently, whenever a user was looking for a specific music file, his client software was sending an inquiry to the central indexing server, which then searched through the other users' libraries for matching files. If a match was found, a direct connection was then established between the two PCs, through which the inquiring user downloaded the file.

In principle, Grokster (the P2P software which was a subject of the second case) operated in a similar manner to its predecessor, Napster; with one critical difference. As Boyle noted, the developers of Grokster decided to part with the idea of a central indexing server for the purpose of shielding themselves from liability;[127] in this network, it was the users' own computers which were performing this function. Chosen according to their PC's power, those "user servers" were communicating the file search requests to each other, thus providing for a uniform filesharing network.

It should come as no surprise that both Napster and Grokster became used for sharing music files without the copyright owners' permission. For the purposes of this work, we ought to look at such infringing use through the lens of the same two provisions of the InfoSoc Directive which appeared in the previous sections of the chapter. While both of those P2P networks were subject to litigation in the US jurisdiction, the technology behind them is not, just as the Internet itself, bound by the borders of national legal systems and the EU policymakers should take all possible filesharing networks into account when regulating this area of law.

Starting with art. 2, it seems plausible to state that in case of both Napster and Grokster, reproduction occurred whenever a user, already connected to his "destination" PC, downloaded a copyrighted file to his own hard drive. It is worth to note that the file itself was not reproduced on Napster's indexing server or Grokster server-users' PCs – they merely pointed out the route

[127] Boyle J, *The Public Domain: Enclosing the Commons of the Mind* (YUP 2008), at 76.

towards the right location on the network.

As for art. 3 and the act of communication to the public, it seems fair to say that whenever a user sent his dedicated music library to Napster's central indexing server, he was communicating/making available the files placed within that folder; actions of Grokster's users who contributed copyrighted files to the network followed this pattern. It has to be added that while Grokster's case raises further interesting questions of liability - for example, when we consider "servering" users who automatically helped other users locate the infringing files, it is questionable whether such actions would fall under the scope of art. 3. The exemplified users were not communicating the file itself; it is more accurate to say that they were indiscriminately pointing the direction to the files sought by other users.[128]

Our journey through the realm of various P2P networks continues with the UK case of *Polydor v Brown* (2005)[129] (probably the first UK case dealing with peer-to-peer filesharing), which saw a user of the gnutella P2P network liable for making 400 music files available to other users without seeking the copyright owners' permission.

Gnutella, which was the single most popular filesharing network in 2006/2007 with over 40 % of the ecosystem's activity,[130] has an even more decentralised structure than Grokster, with each user becoming a "node" of the system. In principle, the process here goes as follows; upon downloading a gnutella client software (such as, for example, LimeWire), the user becomes connected to a certain limited amount of other gnutella users. Whenever someone wants to download a specific file, his search request is initially sent to those users he's connected with; should no matching files be detected, the user's request is passed to all users the initial request receivers are connected to. The process continues until a match is found; then, similarly to previous examples, a direct

[128] That being said, the court in the Retroshare case adopted a different line of reasoning; see later in this section.
[129] [2005] EWHC 3191 (Ch).
[130] See http://arstechnica.com/uncategorized/2008/04/study-bittorren-sees-big-growth-limewire-still-1-p2p-app/.

connection is established between the initial user's and the matching result holder's PCs, and the download may commence.

Nevertheless, in terms of the Information Society Directive's articles, gnutella follows the pattern described in relation to both Napster and Grokster. Reproduction occurs when the copy of a copyrighted file is made following its download, and communication to the public occurs upon making the infringing file available to the set of users one is connected to.

Such analysis also applies to the final example of a network described in this subsection; the anonymised filesharing service known as Retroshare.[131] In this P2P network, similarly to gnutella, each user acts as "node" in the system. In 2012, the Hamburg Regional Court ruled that if a situation occurs in which a search request for a copyright-infringing file passes through Retroshare user's computer, this user is liable for the infringing transfer of information[132] – a ruling which is further discussed in chapter two.[133] For now, it suffices to say that the court found the discussed transfer of information to be going against the right of reproduction and the right of communication to the public, as they are set in s. 85(1) of the German Copyright Act 1965.

2.2.4. Copyright-infringing content vs. search results leading to legitimately uploaded, publicly available content.

The factual scenarios presented above, occurring in relation to cyberlockers, streaming websites and P2P networks, fit fairly smoothly within the scope of this thesis; they portray resources used for making infringing content available, content which is often accessed through a variety of indexing services and networks.

However, it cannot be omitted that at times, articles 2 and 3 of the InfoSoc

[131] See http://www.techdirt.com/articles/20121127/13221421157/german-court-holds-internet-user-responsible-passing-unknown-encrypted-file.shtml
[132] The *Retroshare* case (2012) LG Hamburg, 308 O 319/12.
[133] See chapter two, section 2.1.2.

Directive are invoked not against infringing content or the indexing services leading to it, but against various forms of search results leading to perfectly legitimate content, publicly accessible and present on the Web with its copyright owner's blessing. Relying on the examples of image search and news aggregation services, this section aims to show how such atypical situations might arise and to explain why this thesis is not going to cover such patterns of (potential) infringement.

2.2.4.1. Image search engines and legitimately uploaded, publicly available, copyrighted content.

Examples related to the image search engines are going to be presented first – hence, a few words should be said about the basic workings of those services. Their chief representative is Google Image Search – and it is going to serve us as an example. In response to a search query, Google Image Search identifies text in its database responsive to the query and then communicates to users the images associated with the relevant text. Google Image Search provides search results as a list of small images called "thumbnails," which are stored in Google's servers. The thumbnail images are reduced, lower-resolution versions of full-sized images stored on third-party computers. When a user types a search term into Google Image Search, he is presented with a list of thumbnails that Google's algorithms have ranked by relevancy to the search term.

Google Image was the focal point of two German Federal Court of Law cases, which perfectly illustrate the kind of a scenario discussed in this part of the chapter. The first one of them is *Tutsche v Google* (2010),[134] the facts of which were as follows. The claimant uploaded pictures of her own works of art onto her own, publicly available, website. As one could expect, the Google Image search engine located and indexed those files, presenting them among its search results, in the form of thumbnails. The claimant contested that the copyrights she held in those pictures were infringed when the said pictures

[134] Federal Court of Justice, decision dated 29.04.2010 – I ZR 69/08.

became shown as thumbnails.

Germany's Supreme Court dismissed this claim: most significantly, by finding that the claimant has given a specific form of implied consent (referred to as "simple" consent[135]) to the defendant, for the contested processing of her works. In the judge's words: "placing images on a publicly available website, without taking the technological precautions; could be objectively understood by the defendant (Google) as operator of a search engine as a consent that the depictions of the works of the Plaintiff could be used in the image search to the usual extent".[136] The phrase "technological precautions" refers here to the simple act of changing the claimant website's robots.txt file, so that it tells Google Image crawlers not to index its contents (for example, the contested images). It is important to note that the same mechanism applies to Google Search, the US company's primary search engine.

The second case, *Bernhard v Google* (2011),[137] differs from *Tutsche* in that it involves a third party website, where the images were stored; but similarly to the first case, the content was hosted there legitimately. In *Bernhard*, the claimant was the author of a photograph depicting a well-known TV presenter – the said photograph was uploaded onto a third party's website, with the claimant's consent.[138] Since the operators of this website did not take the technological precautions of the kind described in the preceding paragraph, Google Image indexed the photograph in question, together with its derivative thumbnail. The claimant complained that such a thumbnail infringes his rights, primarily the right to make the photographic work available to the public, granted by s. 19(4) of the German Copyright Act.[139]

---

[135] *Tutsche v Google*, supra fn. 134, [28] to [36].

[136] *Tutsche v Google*, supra fn. 134, at [36].

[137] Federal Court of Justice, decision dated 19.10.2011 – LZR 140/10 (also known as the "Vorschaubilder II" case.)

[138] As it turned out, the case also involved the copies of the photograph being uploaded *without* the claimant's consent on further third party websites, but such circumstances fall outside of this section's scope.

[139] Which sets out "(…) the right to make a work of fine art, a photographic work, a cinematographic work, or illustrations of a scientific or technical character perceivable to the public by means of technical devices". (translation obtained from http://www.iuscomp.org/gla/statutes/UrhG.htm#19).

The Supreme Court dismissed this claim for reasons similar to those in *Tutsche* – it was found that by allowing the third party website to host the contested photograph, the claimant gave a specific form of consent for the processing of the work in the Google Image search engine. The key paragraph of the decision states that "an author who posts his works on his Internet-site, without excluding these images from search and display by search engines by means of technical measures, in the view of the operator of a search engine, by conclusive behaviour declares himself in agreement that the search engine will show thumbnails of these images. *It could not be otherwise, when an Author has given permission to a third party to post images of his works on the internet* and when the thumbnails shown by the search engines are based on the images posted on the internet by the said third party".[140] The third party website did not change their robots.txt file in the relevant manner,[141] and the photograph's copyright owner's claim failed.[142]

Both decisions presented above seem to indicate that within the German law, image search engines such as Google Image are not at risk of incurring liability for copyright infringement, assuming the images they index are hosted legally and are publicly available. Moreover, since art. 19 of the German Copyright Act implements art. 3 of the InfoSoc Directive, *Tutsche* and *Bernhard* could be seen as suggesting a potential interpretation of the EU law in the described circumstances. That being said, it is still unclear what would happen if the act of reproduction/communication to the public committed by an indexing service would differ from the thumbnail system used by Google Image.

2.2.4.2. News aggregation services and legitimately uploaded, publicly available, copyrighted content.

The second category of online resources covered in this section are news

[140] Vorschaubilder II, supra fn. 137, at [9], emphasis added.
[141] Vorschaubilder II, supra fn. 137, at [16].
[142] For further discussion of this case, see Sanders A, 'Intellectual property liability of consumers, facilitators and intermediaries: Comparative Concepts', in Heath C and Sanders A (eds), *Intellectual property liability of consumers, facilitators and intermediaries* (2012), at 7.

aggregation services. The key concept underlying such services is to index news articles from various sources and present them to the subscribers in an easily accessible and customizable manner – in most cases, this includes providing a link to the indexed articles as well. Some of them operate as a search engine hosted on a website (for example, Google News[143]), others provide their customers with similar information by email (for example, Infopaq's software[144]). Each of the bracketed examples became subjected to major litigation proceedings, presented in the following paragraphs.

In the CJEU case of *Infopaq International v Danske Dagblades Forening* (2009),[145] the defendant company ran the following service: whenever a customer sought to find articles concerning a specific topic, he was choosing a relevant keyword(s). He was then provided, by email, with the summaries of matching articles published in the Danish newspapers and other periodicals. Such summaries were accompanied by eleven words-long excerpts of the indexed articles, made of the located keyword, five words following it and five words preceding it. The agency representing the Danish newspapers filed a lawsuit, claiming that a business model of this kind infringes on its members' copyright. The Danish court decided to refer the case to the CJEU.

Infopaq's news aggregation service was regarded by the Court as "reproducing" a substantial part of the copyrighted articles (within the meaning of art. 2 of the InfoSoc Directive), through the inclusion of the earlier mentioned eleven words-long excerpts. It was stated that "the reproduction of an extract of a protected work which, like those at issue in the main proceedings, comprises 11 consecutive words thereof, is such as to constitute reproduction in part within the meaning of Article 2 of Directive 2001/29, if that extract contains an element of the work which, as such, expresses the author's *own intellectual creation*".[146] Following this ruling, the Danish Supreme Court found that some of those eleven words-long excerpts are most likely going to contain an element of intellectual creativity, and decided that

[143] Available at http://news.google.com/.
[144] See http://www.infopaq.com/.
[145] Case C-5/08 *Infopaq International A/S v Danske Dagblades Forening* [2009].
[146] *Infopaq*, supra fn. 145, at [48].

Infopaq requires a licence from the relevant copyright owners in order to continue its business activity.[147]

The second case presented here for the purpose of showing how news aggregation services are targeted by copyright owners for providing access (in various forms) to publicly, legitimately available content is *Copiepresse v Google* (2011).[148] Google News, the service which lied at the heart of the case, functions in the following manner. Firstly, the website indexes articles from thousands of selected publishing websites. Whenever a user accesses Google News, he receives information on the articles related to the topic, location, etc. of his choice. This information is presented in the form of search results consisting of the article's title, the first two-three lines of its text and, depending on the availability, a thumbnail of the main picture attached to the article.

The claimant, an agency representing the interests of Belgian news publishers, brought a case against Google News on two grounds. Firstly, it claimed that Google News presents a substantial part of Copiepresse members' articles, thus infringing their right of reproduction and right of communication to the public, protected by the InfoSoc Directive. The second claim (less relevant for this section of the chapter) was related to Google Search, and stated that this service is breaching Copiepresse members' copyright by storing cached copies of the articles, what prevents the copyright owners from amending or removing them.

The judgment of the Court of Appeal of Brussels found the case for the claimants. It was decided that Google News' activity breaches the claimant's copyright, and Google is not obtaining the news publishers' implied consent by relying on the opt-out scheme based on news publishers amending their websites' robots.txt files,[149] in the manner described above.[150] Google was

[147] The decision (in Danish) is available at http://www.domstol.dk/hojesteret/nyheder/Afgorelser/Documents/97-2007.pdf.
[148] *Copiepresse v Google Inc.* [2011] 2007/AR/1730, at the Brussels Court of Appeal, 9th Chamber.
[149] *Copiepresse v Google Inc*, supra fn. 148, at [50].

ordered to remove the claimants' articles from the Google News service, together with their cached copies stored by Google Search.[151][152]

2.2.4.3. Conclusion.

Looking back at the presented case law, it seems plausible to assume that image search engines can operate legally within Germany (and potentially, the EU), and that some news-aggregation services active in the EU may, in certain circumstances, be required to obtain a licence from the relevant copyright owners; something that is difficult to reconcile with the fact that the said owners are rarely eager to complain about the additional traffic they receive from such schemes.

However, as one might notice, the legal questions raised in the described scenarios differ from the questions this thesis is focused upon. The latter questions are tied to the concept of infringing content, content which is deemed to be undesirable and should not be accessible in cyberspace, unless the respective rightholders wish for it. Cases such as *Bernhard*, *Tutsche*, *Infopaq* and *Copiepresse* have a different focus, they are primarily asking about the legitimacy of business models utilising publicly available, legitimate content; about the form in which such services should present the content they index. Those cases are not concerned with phenomena such as the whack-a-mole game played with copyright-infringing content spreading through cyberlockers, streaming websites or P2P networks.

For those reasons, copyright enforcement attempts aimed at services indexing legitimate, publicly available, online content are not covered in this dissertation. That being said, enforcement schemes aimed at indexing services

---

[150] See the decisions described in section 2.2.4.1.
[151] *Copiepresse v Google Inc*, supra fn. 148, at [66].
[152] For further discussion of news aggregation services, see, for example, *Public Relations Consultants Association Ltd v Newspaper Licensing Agency Ltd* [2013] UKSC 18, as well as the German ancillary copyright bill, commented on in Barabash I - 'Ancillary copyright for publishers: the end of search engines and news aggregators in Germany?' (2013) E.I.P.R. 35(5), 243, at 245. A similar act of the Spanish parliament - Ley 21/2014, de 4 de noviembre, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual - can be indicated here as a key point of reference as well.

used for spreading infringing content *per se* are well within its scope; such schemes are covered in chapter two.

3. Trademark-infringing content.

3.1. European Union's legal framework governing the identification of trademark-infringing content.

Similarly to copyright law, the law of trademarks also became significantly regulated on the EU level, through (*inter alia*) the introduction of specific harmonised rights granted to the trademark owners within the Community. First of all, just as it was with copyright, protection of trademarks within the EU law is enshrined in art. 17(2) of the Charter of Fundamental Rights of the EU, which recognises the protection of intellectual property rights as a part of the fundamental right to property.[153] Furthermore, when it comes to trademarks in the EU, the principle of IP protection extends to both Member States' national trademarks and the Community trade mark, established by art. 1(1) of the Community Trademark Regulation 40/94.[154]

This two-fold protection comes to life in the form of the harmonised right to use the trademark in the course of trade. On the international stage, it is set out in art. 16 of the TRIPS Agreement 1994, which states that:

"The owner of a registered trademark shall have the exclusive right to prevent all third parties not having the owner's consent from using in the course of trade identical or similar signs for goods or services which are identical or similar to those in respect of which the trademark is registered where such use

[153] CFREU, supra fn. 7.
[154] Council Regulation (EC) No 40/94 of 20 December 1993 on the Community trade mark, art 1(1) (as renewed by the Council Regulation (EC) No 207/2009 of 26 February 2009 on the Community trade mark, art. 1(1).)

would result in a likelihood of confusion. In case of the use of an identical sign for identical goods or services, a likelihood of confusion shall be presumed".[155]

Moving back to the EU, a discernible connection can be found between this provision and the wording of the European legal instruments creating a harmonised right to use in the course of trade for both national and Community trademarks. Firstly, art. 5 of the Trademarks Directive 89/104[156] (as renewed by the Directive 2008/95[157]) bestows upon the national trademark owners the right to prevent others from using in the course of trade:

- "any sign which is identical with the trade mark in relation to goods or services which are identical with those for which the trade mark is registered",[158]
- "any sign where, because of its identity with, or similarity to, the trade mark and the identity or similarity of the goods or services covered by the trade mark and the sign, there exists a likelihood of confusion on the part of the public, which includes the likelihood of association between the sign and the trade mark"[159], as well as:
- "any sign which is identical with, or similar to, the trade mark in relation to goods or services which are not similar to those for which the trade mark is registered, where the latter has a reputation in the Member State and where use of that sign without due cause takes unfair advantage of, or is detrimental to, the distinctive character or the repute of the trade mark".[160]

[155] TRIPS, supra fn. 10, art. 16.
[156] Directive 89/104/EEC of 21 December 1988 to approximate the laws of the Member States relating to trade marks, art. 5.
[157] Directive 2008/95/EC of the European Parliament and of the Council of 22 October 2008 to approximate the laws of the Member States relating to trade marks, art. 5.
[158] Trademarks Directive, supra fn. 156, art. 5(1)(a).
[159] Trademarks Directive, supra fn. 156, art. 5(1)(b).
[160] Trademarks Directive, supra fn. 156, art. 5(2).

Following this provision, art. 9 of the earlier mentioned Community Trademark Regulation grants the mirrored version of this right to bearers of the Community trademark.[161]

3.2. Factual scenarios leading to the transfer of trademark-infringing content.

Both manifestations of the harmonised right to use in the course of trade are liable to be infringed in cyberspace, in a variety of ways. In recent years, courtroom battles occurred over the use of trademarks in scenarios involving domain names,[162] online banners and metatags,[163] as well as keyword advertising.[164] For the purpose of this thesis, focused on the infringement of various legitimate interests by means of digital content (especially that which is shared by the users of online services), two modes of online trademark infringement seem to be of particular relevance – namely, the spread of digital content aimed at facilitating the trade in counterfeit goods and impersonations of popular persons and companies on social websites. Described below are three cases demonstrating the occurrence of such infringing activities through the use of different online services.

3.2.1. Auction websites.

First of them is the landmark decision of the CJEU in the case of *L'Oréal v eBay* (2011).[165] eBay is an online marketplace website, which allows its users to sell and buy a nigh-endless variety of products from each other, with eBay's revenue coming from a percentage fee collected after each completed transaction. As time passed, eBay became used by sellers of counterfeit goods,

[161] Community Trademark Regulation, supra fn. 154, art. 9.
[162] For example, Case C-569/08 *Internetportal und Marketing GmbH v Schlicht* (2010).
[163] For example, *Reed Executive Plc v Reed Business Information Ltd* [2004] EWCA Civ 159.
[164] For example, Case C-236/08 *Google France SARL v Louis Vuitton Malletier SA* (2010).
[165] Case C-324/09 *L'Oréal SA v eBay International AG* (2011).

especially those bearing the trademarks of companies producing luxury goods. One of such companies, L'Oréal, sued eBay for facilitating the trade in goods infringing their trademark. While the Court's decision in this case is described in more detail in chapter two,[166] in this subsection, it is sufficient to say that the Court found that counterfeits of L'Oréal's products were indeed sold on the defendant's website (a finding confirmed by eBay), and this constituted an activity breaching the harmonised right to use in the course of trade, as set out in Directive 89/104 and Regulation 40/94.[167]

3.2.2. Website chains.

The second case covered in this subsection is the US 9th Circuit Court of Appeal's decision in *Louis Vuitton v Akanoc Solutions* (2011).[168] It does not match the previous case in terms of thesis-relevant, jurisdictional authority, but it presents a different, complex mode of trademark infringement, which provides a good contrast to the factual background of the *L'Oréal* case. In *Akanoc*, the following chain of trademark infringement was the subject of a legal dispute: consumers were visiting special websites, which instead of selling merchandise, hosted email addresses of Chinese companies making and distributing LV counterfeit products. Those websites leased server space, bandwidth and IP addresses from Akanoc, which in turn leased those assets from another company called MSG – interestingly enough, both Akanoc and MSG were owned by the same person. LV sent notices of infringement to both Akanoc and MSG, demanding the removal of access to infringing websites, but these notifications were ignored. In the end, the defendants were found to be liable for contributory trademark infringement, a fact which leaves little space for questioning the presence of the infringing use of the website in question, as it is likely that the same set of facts (which might, after all, come to occur within the European Union) would be considered to involve a breach of the harmonised right to use in the course of trade in the EU.

---

[166] See chapter two, sections 3.1.2.2, 3.1.1.1, and 3.3.1.2.
[167] *L'Oreal v eBay* (CJEU), supra fn. 165, at [H6].
[168] US CoA 9th Cir. 10-15909.

3.2.3. Social media.

A case demonstrating the impersonation-centred infringement of a trademark could be the "Exxon Janet" incident,[169] where a user known as Janet created a Twitter account named Exxon Mobil Corp, and pretended to be an employee of the corporation. "She" actually provided false answers to the users' questions about Exxon's philanthropic policies.[170]

It is uncertain whether such an activity could be covered by the expression "using in the course of trade". When analysing this matter from the US angle, Ramsey stated that "it is unclear whether trademark infringement law applies where the mark is not being used to advertise or sell goods or services";[171] and this statement holds true for the EU as well. Should it be reasoned that Exxon Janet was actually performing a service identical to that performed by the oil company (answering the public's queries), the content she produced could be seen as infringing art. 5 of the Trademarks Directive, for the likelihood of confusion was clearly present in the discussed scenario. That being said, this situation could also be seen as involving defamatory content, which is covered in section 5 of the current chapter.

4. Privacy-infringing content.

4.1. European Union's legal framework governing the identification of privacy-infringing content.

[169] See http://www.computerworld.com/article/2532609/web-apps/exxon-mobil-s-brand--hijacked--by-impersonator-on-twitter.html

[170] See also *Oneok, Inc. v Twitter, Inc.* (2009) (Complaint) – accessible at http://www.dmlp.org/sites/citmedialaw.org/files/2009-09-15%20-%20ONEOK%20Complaint.pdf

[171] Ramsey L, 'Brandjacking on Social Networks: Trademark Infringement by Impersonation of Markholders' (2010) Buffalo Law Review 58, at 854.

The third category of infringing content which is going to be covered in this thesis is privacy-infringing content. Before moving on to the European Union's legal instruments defining this category, it is worth looking towards two international documents, which greatly influenced the shape of the EU's legal instruments aimed at protecting its citizens' privacy. Firstly, art. 12 of the Universal Declaration of Human Rights (hereafter referred to as the UDHR) states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence [...]. Everyone has the right to the protection of the law against such interference or attacks".[172] The UDHR influenced the composition of the array of rights set out in the European Convention on Human Rights (hereafter referred to as the ECHR); among them, the right to respect for private and family life. This right is set out in art. 8 of the ECHR, which states that "everyone has the right to respect for his private and family life, his home and his correspondence".[173] In 2000, this right was enshrined (in a slightly altered form) into the EU law by the Charter of Fundamental Rights of the European Union (hereafter referred to as the CFREU or the Charter), art. 7 of which provides that "everyone has the right to respect for his or her private and family life, home and communications".[174]

This covers the general, overarching aspect of the EU right to privacy and its historical underpinnings. However, the rapid progress of information technology in the second half of the twentieth century prompted the development of a specific, (arguably) secondary right, aimed at protecting the EU citizens' privacy in the digital age; the right to protection of personal data. Over the years, it became enshrined in both CFREU (art. 8(1) of which states that "everyone has the right to the protection of personal data concerning them"[175]) and the Treaty on the Functioning of the European Union (hereafter referred to as the TFEU) (which mirrors art. 8(1) of the Charter, save for the

[172] Universal Declaration of Human Rights 1948, art. 12.
[173] European Convention on Human Rights 1950, art. 8(1).
[174] CFREU, supra fn. 7, art. 7.
[175] CFREU, supra fn. 7, art. 8(1).

switch from "him or her" to "them".[176]) It should be noted that as a matter of fact, the discussion over the nature of the relationship between data protection and the right to privacy is far from settled – as section 2.2 of chapter four demonstrates.

The key legal instrument governing the operation of this right in the EU is the Data Protection Directive 95/46[177](hereafter referred to in this subchapter as "the Directive"). Art. 1 obliges the Member States to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data".[178] The two key terms of this provision, "personal data" and "processing", are expanded in art. 2 of the Directive, with the former broadly defined as "any information relating to an identified or identifiable natural person"[179], and the latter described in a similarly general manner as "any operation or set of operations which is performed upon personal data".[180]

The Directive creates a set of rights aimed at securing the objective furthered by its first article. One of them in particular merits the attention of this thesis; the right to rectification, erasure or blocking set out in art. 12(b) of the Directive, which states that:

"Member States shall guarantee every data subject the right to obtain from the controller:

- (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this

[176] Treaty on the Functioning of the European Union, art. 16(1).
[177] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[178] Data Protection Directive, supra fn. 177, art. 1.
[179] Data Protection Directive, supra fn. 177, art. 2(a).
[180] Data Protection Directive, supra fn. 177, art. 2(b).

Directive, in particular because of the incomplete or inaccurate nature of the data;"[181]

Out of various provisions of the Directive capable of triggering this right, the focus of this thesis warrants giving attention to art. 7(a), which states that personal data may be processed only if "the data subject has unambiguously given his consent".[182]

The Data Protection Directive has been updated and complemented on quite a few occasions,[183] much in the spirit of art. 5, which provides that Member States shall "determine more precisely the conditions under which the processing of personal data is lawful".[184] The most recent attempt of this kind is the European Commission's proposal of the General Data Protection Regulation[185] (hereafter referred to as "GDPR"), which (among other things) aims to take the right provided by the art. 12(b) of the Directive further, through the creation of the right "to be forgotten and to erasure". It is set out in the art. 17 of the proposal, in the following shape:

"The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:"[186]

[181] Data Protection Directive, supra fn. 177, art. 12(b).
[182] Data Protection Directive, supra fn. 177, art. 7(a).
[183] Most notably, by the Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, and the 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 (Directive on privacy and electronic communications).
[184] Data Protection Directive, supra fn. 177, art. 5.
[185] Proposal of the General Data Protection Regulation 2012/0011.
[186] GDPR proposal, supra fn. 185, art. 17.

Out of four listed grounds, the one set in art. 17(b) is of particular significance, as it is connected to the earlier mentioned art. 7(a) of the Directive. The proposed provision would enable the right to be forgotten and to erasure where:

"the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1),[187] or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;"[188]

As the Commission's proposal has not been adopted yet, this thesis endorses the Data Protection Directive as the key point of reference. The cited provisions of the GDPR might also, at the time of writing, still change – for example, the European Parliament's Albrecht Report proposed a sizeable amount of amendments to this document, such as dropping the reference to childhood in art. 17.[189]

4.2. Factual scenarios leading to the transfer of privacy-infringing content.

There can be little doubt about the validity of the statement made by Lord Hoffmann in the case of *R v Brown* (1996),[190] where he expressed his concern over the erosion of privacy by means of the developing information technologies, stating that "the right to keep oneself to oneself, to tell other

[187] Which states that "processing of personal data shall be lawful only if and to the extent that at least one of the following applies: (…) the data subject has given consent to the processing of their personal data for one or more specific purposes;".
[188] GDPR proposal, supra fn. 185, art. 17(b).
[189] Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), at 95.
[190] [1996] A.C. 543.

people that certain things are none of their business, is under technological threat".[191] Indeed, the prime example of such technologies, the cyberspace, provides for a variety of ways in which one's privacy might be encroached upon; for example through being tracked online by websites (for example, through cookies,[192] and/or with a geolocational element[193]), being a victim of spyware,[194] or being a subject to data mining[195] activities. While those examples undoubtedly merit academic attention, this thesis (focused on the infringing content, especially in its user-generated aspect) is going to focus on different scenarios of online infringement, presented in the following paragraphs.

These are divided into two parts; the first one presents three different incidents of potential privacy infringement via digital content shared online, and follows on to analyse them in the light of the legislative instruments described in section 4.1. The second part focuses on the CJEU case of *Google Spain v Mario Costeja Gonzalez*[196] (hereafter referred to as the *Costeja* case) which deserves to be dealt with separately, for it obscures the division between the concept of the infringing content and the search results leading to content which was legitimately uploaded and is publicly available. Finally, it should be remembered that the factual scenarios presented below are not forming an exhaustive list of all potential ways through which privacy could be infringed by digital content shared online. For example, a privacy-infringing video/sound recording/text could be shared through all of the platforms used for sharing copyright-infringing content which are described in section 2.2 of this chapter.

---

[191] *R v Brown*, supra fn. 190, at 556.

[192] In an outline, cookies are small files placed by websites on their visitors' computers. Such files may record the elements of the user's browsing history, as well as other browsing data (such as recorded logins and passwords).

[193] Such an element comes to play when we consider, for example, the geolocational data produced by a smartphone user.

[194] The term spyware denotes various categories of malicious software aimed at - among others - extracting information from the targeted party without the latter's knowledge.

[195] Data mining is, in a broad sense, an activity consisting of gathering and analysing data from various sources in order to obtain further information resulting from the integration of the said resources. When data mining is performed on various sources of personal data, it becomes a potential problem for privacy and data protection legislation.

[196] Case C-131/12 *Google Spain v Gonzalez*.

4.2.1. Facebook, Twitter and streaming websites.

The first incident covered in this section is related to a Facebook group page which was known as the "Whores of Antwerp".[197] Its appearance confirms the statement made by Gonzalez in his article from 2012, where he wrote that "every time a new user joins an online network and provides his personal data and posts personal photos or comments, he is not only extending and reflecting part of his personality but also exposing it to the ravages of the digital world".[198] The Facebook group in question was set up by a group of teenagers, who were befriending girls using this social network, copying the latters' pictures onto the group page, and adding annotations such as "prostitute", "cocaine sniffer" and "hot wench". While this case could clearly be used as an example in the defamation subchapter, the fact that the perpetrators were taking girls' photos out of their "network of friends" and maliciously putting them onto the public Facebook group, suggests its potential for privacy-infringing implications.

The second scenario is arguably even more harmful and malicious than the activity described in the previous paragraph, for it revolves around the phenomenon of "revenge pornography" and revenge pornography websites, such as IsAnybodyDown. The owner of this website posted "revealing pictures, mostly of women, without their consent, along with their full names and identifying information like phone numbers and Facebook snapshots".[199] Should a victim desire to remove such content from the website, they were directed to a "takedown service", which carried a charge of $250. The term "revenge pornography" comes from the notion that the content in question might often be provided by the victim's ex-boyfriend or ex-girlfriend, who

[197] See (http://www.expatica.com/be/news/belgian-news/Antwerp-whores-Facebook-fan-page-under-investigation-_254445.html).
[198] Gonzalez L, 'Habeo Facebook ergo sum? Issues around privacy and the right to be forgotten and the freedom of expression on online social networks' (2013) Ent. L.R. 83, at 83.
[199] See (http://arstechnica.com/tech-policy/2013/02/revenge-porn-is-just-entertainment-says-owner-of-isanybodydown/).

wishes to take revenge on them; this introduces the web 2.0 element to the equation.

Contrary to the first two examples, the third scenario of infringement is based on an actual legal case, quite well-known in the UK - *CTB v News Group Newspapers* (2011).[200] To summarise the events which led to the court room; first of all, *The Sun* newspaper published an article indicating that a female model and celebrity known as Imogen Thomas had an affair with an unnamed footballer – who, as it is well known at this point, turned out to be Ryan Giggs. Ms Thomas blackmailed him, demanding considerable amounts of money in return for not selling the story of their affair to the newspaper. This is where the gist of this scenario begins; Giggs successfully applied for a preliminary injunction, preventing not only the newspaper, but anyone in the UK from publishing statements which would identify him as the unnamed footballer. However, this information was leaked, and soon enough, various social media websites (most notably, Twitter), were buzzing with the information that Giggs is the footballer who had an affair with Ms Thomas.[201] One of the significant aspects of this case is that initially, the potentially infringing content did not emerge on the web 2.0 websites - but they played a key part in making it public.

With all three scenarios described, it is time to consider whether the digital content lying at the heart of each of them could be classified as privacy-infringing content, access to which should be removed. Starting with the broad notion of privacy, it seems plausible to state that in each of the three cases, the victim's right to "respect for his or her private and family life, home and communications," as provided by art. 7 of the CFREU, was infringed. With this said, we can move towards the data protection legislation, and the question of whether the content which was contested in those incidents can be

[200] [2011] EWHC 1232 Q.B.
[201] What led to serious questions about the effectiveness of such an injunction – see section 2.1 of chapter three.

classified as personal data within the meaning of the Data Protection Directive, as well as the proposed GDPR.

First of all, as Kuschewsky notes, the proposed regulation does not refer explicitly to the responsibility of the individuals who post data without the data subject's consent[202] - and nor does the Directive. That being said, there are fairly convincing arguments for recognising the privacy-infringing content in the three cases as "personal data," under both the Directive and the GDPR; most notably, the decision in the CJEU case of *Lindqvist* (2003).[203] The relevant passage (which also covers the notion of "processing") states as follows:

"the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes "the processing of personal data wholly or partly by automatic means" within the meaning of Article 3(1) of Directive 95/46".[204]

Moreover, regarding the "Whores of Antwerp" case specifically; as Gonzalez rightly points out, "the mere fact that private information is made available to a determined public does not entail that such data have lost their attributes as private information and even less that it can be granted the same usage of public information".[205] The fact that those girls shared their pictures and personal information with a selected group of friends does not strip such content of the "private and personal data" status.

[202] Kuschewsky M, 'The right to be forgotten – the fog finally lifts' (2012) P. & D.P. 10, at 12.
[203] Case C-101/01 *Bodil Lindqvist* [2003].
[204] *Bodil Lindqvist*, supra fn. 203, at [27].
[205] Gonzalez, supra fn. 198, at 87.

Assuming on those grounds that all three cases have involved the processing of personal data within the meaning of both art. 1 of the Data Protection Directive and art. 17 of the GDPR, the following question appears: could the discussed content be subjected to the right to rectification, erasure or blocking set out in art. 12(b) of the Directive, and to its counterpart set out in art. 17 of the Commission's proposal? Art 12(b) is triggered where the processing of data is not compliant with the provisions of the Directive – and if we look back to art. 7(a) of the same legal instrument, it requires that the data subject must have clearly given his or her consent to the processing. It is fairly obvious that this was not the case in any of the scenarios described above. Moreover, art. 17(b) of the GDPR would be *at least* as likely to be triggered by them, due to its reference to the "withdrawal" of consent and – regarding the Whores of Antwerp case - the emphasis placed on protecting children.

4.2.2. Privacy-infringing content vs. search results leading to legitimately uploaded, publicly available content; the *Costeja* decision.

It turns out that the notion of rightholders attempting to remove the access to search results leading to legitimately uploaded, publicly available content - which was discussed in section 2.2.4 in the context of copyrighted content - is not limited to intellectual property; as the case of *Costeja*[206] shows. This preliminary reference to the CJEU came from Spain, and centred around the question of whether search results appearing on Google's search engine as a result of typing in an individual's name and leading to content containing personal data, can be ordered to be removed on the basis of art. 12(b) of the Data Protection Directive,[207] even if the content in question was lawfully published. The claimant on behalf of whom the Spanish data protection authority demanded the removal of such indexing information was a man whose home repossession notice (drawn for non-payment of social security) kept appearing in Google's search results (tied to the claimant's name), as a

[206] *Costeja*, supra fn. 196.
[207] *Costeja*, supra fn. 196, at [100(3)].

part of an indexed article from an online version of the La Vanguardia newspaper.[208]

The Court answered the referred question affirmatively, stating that "the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful".[209]

This case is different from the previous scenarios described in this chapter in that it is not the "source" data itself which constitutes "infringing content"; it is the list of search results displayed after a search on the person's name that links to such a source (for example, a newspaper article): the source being, potentially, uploaded legitimately and publicly available. This leads to a certain paradox - the supposedly undesired content might continue to be accessible regardless of the described removal order. It seems plausible to think that the claimants in such a case might be trying to remove the search results due to their inability to legitimately take down the source of the content: a risk which did not appear in relation to the earlier described copyright scenarios involving news aggregation and some image search cases.

Writing of which: one could wonder why the list of search results from *Costeja* can be seen by this thesis as a peculiar category of infringing content, while the similar information tied to scenarios described in section 2.2.4 is not. While there is no sole correct path of distinction, the factor which guided the author's reasoning here was the claimant's intention. This thesis is focused on the removal of access to infringing information, and this is what the claimants in *Costeja*-type cases seek to achieve. On the other hand, the claimants described in section 2.2.4 were more interested in controlling/monetising the

[208] See Opinion of the Advocate General Jaaskinen in Case C-131/12 *Google v Gonzalez*, at [18].
[209] *Costeja*, supra fn. 196, at [88].

access to information; hence, such scenarios were deemed to be too distant from the leading research question of this thesis.

5. Defamatory content.

5.1. Legal framework of England and Wales governing the identification of defamatory content.

In principle, defamation occurs under the law of England and Wales, whenever someone's reputation is unjustly damaged by means of a published statement. According to the classic definition of this tort found in the case of *Sim v Stretch* (1936), such a statement "tends to lower [the claimant] in the estimation of right-thinking members of society generally",[210] which - as it was stated in the case of *Yousoupoff v MGM Pictures Ltd* (1934) – decreases the claimant's chances of "receiving respectable consideration from the world".[211] That being said, over the recent years, the required threshold of injury to claimant's reputation has been raised, most notably by s. 1(1) of the Defamation Act 2013, which states that a statement will not be regarded as defamatory unless it causes "serious harm to the reputation of the claimant".[212]

Furthermore, the jurisdiction of England and Wales distinguishes two primary modes through which a defamatory statement can be published – libel (which applies whenever the published statement is in written or other permanent form), and slander (which applies to statements passed by spoken word or by other non-permanent form).

[210] [1936] 2 All ER 1237, at 1240
[211] 50 T.L.R. 581; see also *Tolley vs JS Fry & Sons Ltd* [1931] A.C. 333.
[212] Defamation Act 2013 c.26, s.1(1); additionally, s. 1(2) requires that in order to be recognised as having suffered serious harm, "a body that trades for profit" must prove serious financial loss.

5.2. Factual scenarios leading to the transfer of defamatory content.

As in previous subchapters, this section is going to proceed by describing a variety of scenarios where one's reputation is infringed by means of digital content shared through a variety of online services. However, there is one matter of definition which should be dealt with first. As it was mentioned in the previous section, the English law distinguishes between libel and slander – consequently, the first question to be answered is which one of them should apply to the vast world of potentially defamatory digital content in cyberspace? Despite certain notable voices to the contrary (such as the arguments presented in the case of *Smith v ADVFN* (2008)[213]), it is now fairly clear that digital content is perceived as permanent enough to be covered by libel. This assumption is in fact well established by s. 166 of the Broadcasting Act 1990, which states that "for the purposes of the law of libel and slander the publication of words in the course of any programme included in a programme service shall be treated as publication in permanent form".[214] While, as Collins notes, this provision is not often mentioned by the judges, it seems to be quite visible in their decisions.[215]

5.2.1. Traditional media in cyberspace – online newspapers and articles.

When the article, one of the principal forms of written expression, entered cyberspace and webpages therein, and later on, when newspapers from the offline world opened online gateways to their content, defamation claims have naturally followed suit. While it is true that videos, images or even PC games all have a potential to carry defamatory information, an undisputed majority of online defamation claims made in the English jurisdiction seems to be related to text-based forms of expression: starting with the articles posted on both

[213] [2008] EWHC 1797, at [16].
[214] Broadcasting Act 1990 c. 42, s. 166.
[215] Collins M, *The Law of Defamation and the Internet* (OUP 2010, 3rd ed.), at 51.

commercial and independent websites. This section presents two examples of such claims.

In the case of *Jameel v Dow Jones & Co Inc* (2005),[216] an article was posted on the website of the Wall Street Journal Online, implying that the claimant might have been funding/supporting the activities of Al-Qaeda. While the claim ultimately failed due to the finding that no real and substantial tort was committed (only five people were proven to have read the defamatory content, which minimised the damage to reputation),[217] the case retains its potential as an example of how defamatory content can spread through the cyberspace in the form of a news article; and the same applies to the second case covered in this section, *Al-Amoudi v Brisard* (2007).[218] By coincidence, this was also a case related to Al-Qaeda – the defendant published an article on his website, which implied that the claimant was one of the financial supporters of Osama Bin Laden. In this particular action, the claimant wished to obtain a confirmation from the court, stating that whenever the defamatory article is published online, it should be assumed that a substantial (enough) number of people accessed it – a goal which he did not achieve.[219]

5.2.2. Blogs.

The line between blog posts and articles published on websites described in section 5.2.1 can be quite thin – nevertheless, it is worth to deal with the former category separately, for two reasons. Firstly, blogs are traditionally much more closely related to the phenomenon of user-generated content, with websites such as Blogger[220] providing their users with blog hosting services. Secondly, blogs are much more often equipped with comment-making

[216] [2005] QB 946.
[217] *Jameel v Dow Jones*, supra fn. 216, at [55].
[218] [2007] 1 WLR 113.
[219] *Al-Amoudi v Brisard*, supra fn. 218, at [37].
[220] Available at blogger.com.

facilities – and, as it will be shown, those comments may contain defamatory material themselves.

The first case used as an example in this section is *Davison v Habeeb* (2011),[221] which concerned a blog post implying that the claimant was part of a fraudulent and corrupted conspiracy[222] – a theme which often appeared on the defendant's blog (which, it is worth adding, was hosted on blogger.com). While the defamatory potential of the contested statement was not challenged, the case itself focused on the service provider's liability, a subject which falls under the scope of the second chapter of this thesis. Nevertheless, it is worth adding that the claimant failed to prove that she has been on the receiving end of a "real and substantial tort" (again, only five people were proven to have accessed the defamatory statement).[223]

The second and third case are a testament to the earlier mentioned statement regarding the defamatory capability of comments on blog posts. In *Kaschke v Gray* (2010),[224] a defamatory comment was made on a political blog, implying that the claimant could have been involved with the Baader-Meinhof gang.[225] And in the case of *Tamiz v Google* (2013),[226] defamatory blog comments alleged that the claimant's political career was obstructed due to the indecent statements he was supposed to make in relation to women.[227] The blog in the latter case was also hosted on blogger.com.

5.2.3. Online forums and discussion boards.

[221] [2011] EWHC 3031 (QB).
[222] *Davison v Habeeb*, supra fn. 221, at [24].
[223] *Davison v Habeeb*, supra fn. 221, at [27].
[224] [2010] EWHC 690 (QB).
[225] *Kaschke v Gray*, supra fn. 224, at [3].
[226] [2013] EWCA Civ 68.
[227] *Tamiz v Google*, supra fn. 226, at [5].

The key feature distinguishing this category of online resources (which might be used for spreading defamatory material) from the previous ones is a difference in infrastructure, exhibited by platforms such as online forums, message boards and independent Internet discussion systems, such as Usenet.[228] It is perhaps this infrastructure, oftentimes providing a greater degree of anonymity, which prompted various individuals to publish defamatory statements in the following cases.

In the classic case of *Godfrey v Demon Internet Ltd* (2001),[229] a forged posting was shared through the soc.culture.thai Usenet newsgroup by someone pretending to be the claimant. The latter decided to sue the ISP operating the earlier mentioned newsgroup. Next, another Usenet case of *Bunt v Tilley* (2007)[230] saw three defendants sued for the defamatory posts (discrediting the quality of the batteries sold by the claimant) they made on Usenet newsgroups, together with their Internet connection-providing ISPs as co-defendants. Finally, in the case of *Totalise Plc v The Motley Fool* (2001),[231] a certain website provided a discussion board for its members, on which defamatory posts were made (alleging the claimant's insolvency, as well as questioning his managerial competency). The judge found them to be "plainly defamatory statements of a very serious nature".[232]

5.2.4. Social media.

Online services classified as social media (such as Facebook and Twitter) can also be used for spreading defamatory content. Out of various scenarios leading to such an outcome, it is especially worth to look at impersonation cases, which gained a new dimension with the arrival of social media portals, due to the possibility of creating fake profiles and group pages.

[228] For the description of the technology behind Usenet, see section 2.2.3.2 of the current chapter.
[229] [2001] Q.B. 201.
[230] [2007] 1 WLR 1243.
[231] [2001] EWCA Civ 1897.
[232] *Totalise Plc v The Motley Fool*, supra fn. 231, at [H7].

Two defamation cases are presented in the following paragraphs as examples showing how such defamatory content appears on social media websites; *Applause Store v Raphael* (2008)[233] and the "Whores of Antwerp" case, which was discussed previously in this thesis, in the context of privacy infringing content.[234]

In the *Applause* case, the claimant was the owner of a company providing audiences for TV shows. A fake Facebook profile was created under his name, together with a Facebook group set up under the name of the claimant's company (the group was linked to the fake profile).

While the fake profile contained private information, the group (more significantly for this chapter) contained defamatory material. It stated that the claimant borrowed a lot of money and lied about the pay-back dates; none of this was true, and the defamatory character of the posted content was not challenged.[235]

Instead, the defendant tried to claim that he was not the one who used his PC to create the fake Facebook profile and group. His explanation was that it must have been one of the guests he had in his house at the time of the posting, one he was not acquainted with before. The judge did not accept such a line of defence, stating that the defendant's proposition can only be seen as "utterly far-fetched".[236]

As it was noted in section 4.2.1 of this chapter, the second case, focused around the malicious "Whores of Antwerp" Facebook group, includes a defamatory element as well. While posting the girls' pictures and personal details without consent was undoubtedly infringing their privacy, labelling them as prostitutes or drug addicts leads in a straight line to the term "defamatory content".

---

[233] [2008] EWHC 1781 (QB).
[234] The 'Whores of Antwerp' case, supra fn. 197, and section 4.2.1. of this chapter.
[235] *Applause Store v Raphael*, supra fn. 233, [6] and [7].
[236] *Applause Store v Raphael*, supra fn. 233, at [62].

Chapter 2 - Enforcement schemes aimed at the removal of access to infringing content.

1. Introduction.

The very idea of regulating the Internet and the content which travels through its veins has been questioned on more than one occasion; among the most notable challenges of this kind is that made by Barlow in 1996. In his "Declaration of the Independence of Cyberspace", he symbolically asks the governments to refrain from regulating the Internet, on account of it being a different world, one which those governments do not understand; one in which the "(…) legal concepts of property, expression, identity, movement, and context do not apply (…)".[237]

A potentially different view on the matter was endorsed by writers such as Goldsmith and Wu, who presented a wide array of ways in which governments can, to a certain extent, affect the transfer of online information[238] or Lessig, who also denied the notion of the Internet's "irregulability"[239] and proposed that human behaviour can still be regulated online through the four "modalities of regulation": laws, social norms, markets, and – most significantly – the code,[240] that is the "architecture" of cyberspace.

If we turn to the area of online regulation lying at the heart of this thesis, that is the removal of access to specified types of infringing content, it is quite

[237] Barlow J, 'A Declaration of the Independence of Cyberspace' (1996), available at https://projects.eff.org/~barlow/Declaration-Final.html
[238] Goldsmith J and Wu T, *Who Controls the Internet? Illusions of a Borderless World*, (OUP 2006), Chapter 5, 65 to 87.
[239] Lessig L, 'Law of the horse: What cyberlaw might teach' (1999) 113 Harvard Law Review 501, at 506.
[240] Lessig, supra fn. 239, at 507.

clear that the governments and rightholders all over the world follow the idea that cyberspace *can be* and *should be* regulated, and that access to the infringing content *can be* and *should be* restricted (the EU and its members arguably being one of the global leaders in terms of such regulatory activity). This thesis adopts both elements of this approach: without forgetting the wide variety of side effects tied to the discussed regulatory efforts (covered in chapters three and four) and the need to step back if the said efforts cause more harm than good.

While the first chapter presented various ways in which infringing content might appear in and spread through the cyberspace, the role of the second chapter is to present the enforcement schemes which have been applied in the EU in order to remove access to such content. However, before this thesis proceeds towards this task, it seems appropriate to underline certain aspects and characteristics of the second chapter:

First and foremost, the term "removal of access" is understood fairly broadly, as a technical manifestation of its underlying goal, which is to prevent/respond to the infringements of the chosen legitimate interests. Hence, the enforcement schemes presented in this chapter include both the ones which are aimed at removing access in a *direct* manner (such as, for example, an injunction asking an intermediary to remove the infringing information[241]) as well as those which pursue this goal in a more *indirect* manner (through, for example, imposing liability in damages on various stakeholders[242] or blocking access to online resources used for spreading infringing content[243]).

Secondly, this dissertation takes the removal of access to infringing content as its principal angle of assessment. In doing so, it is by no means implied that this is the only proper analytical perspective in this area of research – for

[241] See section 3.1.2.1 of chapter two.
[242] See sections 2.1, 2.2, 3.1 and 3.2 of chapter two.
[243] See section 3.1.2.3 of chapter two.

example, one could look at various legal mechanisms aimed at granting adequate compensation to the rightholders whose interests were infringed by means of online content. Removal of access to infringing content is simply the criteria chosen by this particular piece of research, as it focuses on the sources of the problem.

Finally, this chapter presents the enforcement schemes which are subjected to critical analysis in chapters three and four. And in a way, it could be seen as a showcase of the tools from a toolbox labelled "removal of access to infringing content"; with chapter five aimed at choosing the most relevant, integrated set of tools from this toolbox – which, to put it metaphorically, could contain both fine-tuning screwdrivers, as well as heavy lead hammers.

In terms of structure, the second chapter is divided on two primary subchapters. The first one covers the enforcement schemes aimed at the initial infringer, while the second gives attention to the enforcement schemes focused on various intermediaries whose services facilitate (directly or indirectly) the acts of infringement described in chapter one.

2. Enforcement schemes focused on the infringers.

Going after the infringer could be seen as the traditional, almost instinctive way of dealing with online content infringing one's legitimate interest – this subchapter presents various aspects of this enforcement strategy. Section 2.1 starts by discussing the approach based on making the infringer liable on civil law grounds, what can lead to the award of damages and/or the infringer-oriented injunctions. Section 2.2 constitutes a criminal law-focused counterpart of section 2.1, while section 2.3 provides for a slight contrast, for instead of focusing on a specific enforcement scheme, it centres around a challenge common to the schemes described in the first two sections – namely,

identifying the infringer. Subsequently, the "graduated response" enforcement scheme is presented in section 2.4, followed by the last section of this subchapter, focused on the Digital Rights Management systems - section 2.5.

2.1. Subjecting the infringers to civil liability.

2.1.1. Infringer-oriented damages.

Recovering damages through civil litigation can be seen as the traditional way of handling the infringement of the discussed legitimate interests; hence, it seems to be an adequate starting point for the discussion of infringer-oriented enforcement schemes.

In case of copyright and trademarks, the statement about the perceived presence of the enforcement approach based on civil damages is quite likely to fall in line with Moohr's argument that such remedies "more effectively address the real harm that results when an information product is taken: the loss of value to its holder".[244] The situation can be different for privacy and defamation. Writing about the former, Collingwood submitted that "(t)aking a privacy case to open court and exposing private material to an even wider public audience in exchange for only a limited remedy at common law, therefore, smacks of locking the gate after the horse has bolted".[245] However, the very inclusion of civil damages in this thesis indubitably merits some explanation. After all, one might ask; is there a connection between removing access to content and compensating the claimants whose legitimate interests were infringed?

[244] Moohr G, 'The Problematic Role of Criminal Law in Regulating Use of Information: The Case of the Economic Espionage Act' (2002) 80 N.C. L. REV. 853, at 919.
[245] Collingwood L, 'Privacy in Cyberworld: Why Lock the Gate After the Horse Has Bolted?' (2012) European Journal for Law and Technology, Vol. 3, No. 1, at 7.

It is submitted that, at least in theory, such a connection exists; it lies in the idea that the very threat of civil liability in damages might act as a deterrent, preventing the potential infringers from sharing illicit content online – and this concept extends to all types of infringing content considered in this dissertation. Whether we take a Rapidshare user uploading a bootleg copy of a copyrighted movie, a counterfeit trader advertising his goods on eBay, a malicious hacker exposing his victim's personal data on Facebook or a defamatory blog post on Blogger, it seems plausible to assume that none of these individuals is likely to be keen on paying a hefty sum of money for his/her actions. Thus, access to the infringing content might not take place, as a result of the civil laws warranting the award of damages.

In terms of the European Union's law, the direct legal basis allowing the relevant rightholders to recover civil damages in the described scenarios of infringement exists exclusively within the copyright and trademark sectors of this thesis. Art. 8(2) of the InfoSoc Directive obliges each Member State to "ensure that rightholders whose interests are affected by an infringing activity carried out on its territory can bring an action for damages (…)".[246] Art. 13 of the Enforcement Directive expands this obligation to trademark owners and details the criteria under which an infringer can be sued for damages, by stating that:

- "Member States shall ensure that the competent judicial authorities, on application of the injured party, order the infringer who knowingly, or with reasonable grounds to know, engaged in an infringing activity, to pay the rightholder damages appropriate to the actual prejudice suffered by him as a result of the infringement".[247][248]

[246] Information Society Directive, supra fn. 8, art. 8(2).
[247] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, art. 13.
[248] It is worth adding here that the term "infringer", as used in this provision, could cover both "primary" infringers as well as intermediaries whose conduct was classified as infringing the relevant IP rights.

Among the intellectual property-related scenarios presented in chapter one, the case of *Polydor v Brown*[249] stands as an example of the enforcement scheme described in this subchapter.[250] The filesharing defendant tried to build his defence on the idea that "that he did not know that he was doing anything wrong or illegal, and only let his children download music for themselves".[251] However, the judge dismissed this line of reasoning, stating that "ignorance is not a defence"[252] to the breach of the right of communication to the public (set in s. 20 of the Copyright, Designs and Patents Act 1988[253] (hereafter referred to as the CDPA 1988)), and found the defendant liable in damages.[254] It is worth adding that this case was a part of a larger operation conducted by the British Phonographic Industry (hereafter referred to as the BPI), through which 139 copyright-infringing filesharers were sued by the organisation. The case of *Polydor v Brown* is somewhat an exception here, for the majority of those cases were settled (with the settlement payments reaching up to £6,500).[255]

At this point, it is worth mentioning the existence of law firms such ACS:Law, which pursue (in this company's case, pursued) filesharing infringers in a rather controversial and potentially exploitative manner. Employees of ACS:Law were accessing certain P2P platforms, logging the IP addresses of the alleged infringers, which they then used to obtain court orders forcing the ISPs to reveal the alleged infringers' identities[256] – which is pretty much what BPI did in order to establish their cases. However, ACS:Law's activity differed from BPI's in several aspects.

[249] *Polydor v Brown*, supra fn. 129.
[250] For the analysis of *Polydor v Brown*, see chapter one, section 2.2.3.3.
[251] *Polydor v Brown*, supra fn. 129, at [10].
[252] *Polydor v Brown*, supra fn. 129, at [10].
[253] Copyright, Designs and Patents Act 1988 c.48, s.20.
[254] It should be noted that s. 20 does not require a specific state of mind from the infringer – the judge's reference to ignorance as not being a defence could be somewhat misleading here.
[255] See http://www.theguardian.com/media/2006/jan/27/newmedia.news.
[256] For further discussion of the challenge of identifying infringers, see section 2.3 of this chapter.

The law firm in question was focused on obtaining "easy" settlement fees, by sending out considerable amounts of infringement letters asking the alleged infringers for £500, under the threat of legal action. This assumption is reinforced by the fact that a substantial number of letters sent out by ACS:Law related to files containing pornographic content – recipients of such letters are less likely to be willing to defend themselves in the court of law, due to the "shame" factor. To make matters worse, it is quite probable that the law firm was inaccurate in the process of identifying the infringers – for example, one of the letters was sent to a seventy-eight years old man who barely knew what the Internet was.[257] Finally, when a group of alleged infringers decided not to settle, but to defend themselves in the courtroom, ACS:Law tried to back out of the proceedings. In a judgment denying this motion, that is the decision in *Media CAT Ltd v Adams* (2011),[258] Judge Birss QC stated that ACS:Law's letters were "misleading"[259] and its overall conduct could "at best, (…) be described as amateurish and slipshod".[260]

Leaving the intellectual property realm for a moment, let us turn now towards defamation. As in the previous subchapter, there is no harmonised legal basis for the recovery of civil damages from the infringers who shared defamatory content online. However, such a basis can be found on the national level – though it will inevitably vary between different Member States. In the jurisdiction of England and Wales, recovering damages from the author of the defamatory statement has always been the traditional, principal remedy applied in order to compensate the damage done to the claimant's reputation. Among the factual scenarios described in section 5.2 of the first chapter of this thesis, the one which included the application of the discussed enforcement scheme is the case of *Applause Store v Raphael*.[261] There, the creator of the fake Facebook profile and group was found liable in damages for libel, which amounted to 20,000 GBP; 15,000 GBP for the damage done to the claimant's

[257] See http://news.bbc.co.uk/1/hi/technology/8481790.stm.
[258] [2011] F.S.R. 29.
[259] *Media CAT Ltd v Adams*, supra fn. 258, at [60].
[260] *Media CAT Ltd v Adams*, supra fn. 258, at [58].
[261] *Applause Store v Raphael*, supra fn. 233.

reputation (this includes aggravated damages for basing the defence on a lie) and 5,000 GBP for the damage done to his company's reputation.[262]

As for the privacy-infringing content, the legal basis for imposing liability in damages on the relevant infringers is not (as in the case of defamatory content) harmonised on the EU level, and differs from Member State to Member State. Taking the prevailing supportive example of this thesis, the jurisdiction of England and Wales, we notice that the enforcement scheme covered in this subchapter might prove to be quite challenging to pin down in the context of privacy. In England and Wales, it was generally accepted that before 1998 there was no direct tort of breaching someone's privacy which could lead to the award of civil damages. However, the introduction of art. 8 of the ECHR[263] into the UK law in 1998 by way of the Human Rights Act 1998[264] (hereafter referred to as the HRA 1998) disrupted the stability of this order of things.

On the one hand, Lord Hoffmann in *Wainwright v Home Office* (2004) stated that "although article 8 guarantees a right of privacy, I do not think that it treats that right as having been invaded and requiring a remedy in damages, irrespective of whether the defendant acted intentionally, negligently or accidentally".[265] On the other hand, the judgment in *Campbell v MGN* (2004) expanded the law of breach of confidence to compensate the damage done to claimant's privacy, with the "right to privacy" being mentioned as an indirect basis for such an expansion.[266]

The debate on the general subject of civil liability for breach of privacy in the UK is much more complex and intense than its summary presented in the preceding paragraphs – readers interested in this debate are invited to consult

[262] *Applause Store v Raphael*, supra fn. 233, at [79].
[263] ECHR, supra fn. 173.
[264] Human Rights Act 1998 c. 42, sections 1 and 2.
[265] [2004] 2 A.C. 406, at [51].
[266] [2004] 2 A.C. 457, at [125].

the sources given below.[267] For the purpose of this subchapter, it is worth drawing attention to one particular element of this puzzle, that is the earlier mentioned decision in *Applause Store v Raphael*.[268] Apart from granting damages in defamation, the court also allowed the claimant to recover damages for the infringement of his privacy, caused by the fact that the Facebook profile and group in question contained personal information, such as the claimant's alleged sexual orientation.[269]

2.1.2. Infringer-oriented injunctions.

The general definition of an injunction, as given by Winfield and Jolowicz, is that it is a "judgment or order of the court restraining the commission or continuance of some wrongful act, or the continuance of some wrongful omission".[270] In theory then, it could be granted against a person who infringed one of the four legitimate interests by means of sharing the infringing information online. Such a person could be, for example, ordered to remove the infringing content from an online service on which it is hosted, and/or be prohibited from reuploading the said content.

In fact, the European legal framework provides a legal basis for such injunctions – though only within the chosen content areas of intellectual property. Art. 8(2) of the Information Society Directive states that within the area of copyright, "each Member State shall take the measures necessary to ensure that rightholders whose interests are affected by an infringing activity carried out on its territory can (…) apply for an injunction (…)".[271]

---

[267] Apart from the two cited cases, see also (among others) *Kaye v Robertson* [1991] F.S.R. 62, *Douglas v Hello!(No. 6)* [2005] EWCA Civ 595 and *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB).
[268] *Applause Store v Raphael*, supra fn. 233.
[269] *Applause Store v Raphael*, supra fn. 233, at [81].
[270] Rogers W, *Winfield and Jolowicz on Tort (Eighteenth Edition)* (Sweet and Maxwell, 2010), at 1070.
[271] Information Society Directive, supra fn. 8, art. 8(2).

The Enforcement Directive broadened this requirement to include intellectual property rights in general (including, significantly enough for this thesis, trademarks), and specified the conditions on which an injunction against the infringer can be granted. Art. 9(1) focuses on the preliminary injunctions, and provides that "Member States shall ensure that the judicial authorities may, at the request of the applicant:

- "(a) issue against the alleged infringer an interlocutory injunction intended to prevent any imminent infringement of an intellectual property right, or to forbid, on a provisional basis and subject, where appropriate, to a recurring penalty payment where provided for by national law, the continuation of the alleged infringements of that right (…)"[272][273]

Additionally, art. 11 of the Enforcement Directive obliges Member States to:

- "(…) ensure that, where a judicial decision is taken finding an infringement of an intellectual property right, the judicial authorities may issue against the infringer an injunction aimed at prohibiting the continuation of the infringement. Where provided for by national law, non-compliance with an injunction shall, where appropriate, be subject to a recurring penalty payment, with a view to ensuring compliance. (…)"[274]

As for the privacy-infringing and defamatory content, the European Union's legal framework does not provide for infringer-orientated injunctions – of course, this does not mean that the national legal systems of the EU member states are devoid of such measures. For example, as Winfield and Jolowicz

[272] Enforcement Directive, supra fn. 247, art. 9(1).
[273] The cited provision goes on to discuss the precise conditions under which the described preliminary injunctions are to be granted.
[274] Enforcement Directive, supra fn. 247, art 11.

notice, there is no reason why an infringer-focused injunction should not be granted within the England and Wales' law of defamation.[275]

However, despite the existence of a legal basis which could allow for infringer-focused injunctions, it seems plausible to state that such injunctions are rarely sought by the rightholders; in all four content areas. There are of course certain exceptions – for example, an injunction of this kind was granted in the earlier mentioned Retroshare case.[276] The defendant in these proceedings was prohibited from sharing the infringing file under the maximum penalty of 250,000 euros.[277] Due to Retroshare's architecture, the injunction actually meant that the defendant could not use the service anymore without taking the risk of breaking the court order; after all, the other users could share the infringing file through his computer.

Nevertheless, it is quite difficult to find similar cases where, for example, an infringer who made the claimant's copyrighted work available in cyberspace through Web 2.0 services is targeted by an injunction preventing him from doing so, or where an individual who released the claimant's personal details on the Net is ordered to prevent them from being shared. With certain exceptions (such as the Retroshare case), it is submitted that regardless of the content area, the rightholders focused their efforts on the intermediary-oriented injunctions[278] (due to their greater perceived effectiveness[279]), what resulted in the development and substantial variety of this branch of online enforcement policy. Therefore, it is the latter category of injunctions which receives the lion's share of this thesis' attention.

2.2. Subjecting the infringers to criminal liability.

[275] Winfield and Jolowicz, supra fn. 270, at 1071.
[276] Described in chapter one, section 2.2.3.3.
[277] Retroshare case, supra fn. 132.
[278] Which are covered in section 3.1.2 of this chapter.
[279] As to whether this is the case, see chapter three.

In addition to civil measures discussed in section 2.2 of this chapter, some of the concerned rightholders can also target the infringers with criminal liability and the measures it calls into action. These include fines, prison sentences and confiscation of property. For the purpose of this thesis, this enforcement scheme can be seen as an augmented version of the scheme based on imposing civil liability on the infringers,[280] with the deterrence effect being (in principle) reinforced due to the potentially harsher penalties and the stigma of criminal law.[281]

At the time of writing, the EU law does not provide a harmonised legal basis for making the relevant infringers criminally liable for their actions - and this state of affairs applies to all four content types. Yet again this does not mean that the discussed enforcement scheme is not present in the Member States' national jurisdictions, or (in certain limited instances presented below) within the international law.

Starting with copyright and trademarks, our first stop in this section of the chapter is art. 61(a) of TRIPS 1994, which obliges the signatories to "provide for criminal procedures and penalties to be applied at least in cases of wilful trademark counterfeiting or copyright piracy on a commercial scale".[282] The measures suggested in this provision include imprisonment, monetary fines, as well as "seizure, forfeiture and destruction of the infringing goods and of any materials and implements the predominant use of which has been in the commission of the offence".[283] Additionally, the article flags up the possibility of applying the described measures "in other cases of infringement of

[280] See the first two paragraphs of section 2.1 of this chapter.
[281] For the discussion of whether this is actually the case, see section 3.1 of chapter three.
[282] TRIPS, supra fn. 10, art. 61(a).
[283] TRIPS, supra fn. 10, art. 61(a).

intellectual property rights, in particular where they are committed wilfully and on a commercial scale".[284]

The World Trade Organisation's (hereafter referred to as WTO) dispute settlement panel attempted to interpret the troublesome expression "commercial scale piracy/counterfeiting" in its report from 2009 in the *China - Measures Affecting the Protection and Enforcement of Intellectual Property Rights* dispute.[285] It defined the said term as "(…) counterfeiting or piracy carried on at the magnitude or extent of typical or usual commercial activity with respect to a given product in a given market"[286] and added that "the magnitude or extent of typical or usual commercial activity relates, in the longer term, to profitability".[287] Interestingly enough, the Panel underlined that it does not take the stance with regards to the question of whether art. 61 applies to "acts of counterfeiting and piracy committed without any purpose of financial gain". [288][289]

So far, art. 61 did not lead to the enactment of a corresponding piece of EU legislation. Despite the legislative initiatives such as the "Proposal for a European Parliament and Council Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights"[290] (hereafter referred to as IPRED) proposed in 2005, criminal enforcement of IP rights is not harmonised on the EU level. This is despite the decision in the CJEU case of *Commission v Council* (2005), which declared that the Community legislature is capable of having a limited competence in the field of criminal law, if the application of "effective, proportionate, and dissuasive" criminal penalties is

[284] TRIPS, supra fn. 10, art. 61(a).
[285] Dispute DS362 *China - Measures Affecting the Protection and Enforcement of Intellectual Property Rights* (2009).
[286] WTO DS362, supra fn. 285, [7.577].
[287] WTO DS362, supra fn. 285, [7.577].
[288] WTO DS362, supra fn. 285, [7.622].
[289] For further examples of international law-related activity in this area, see Council of Europe's Convention on Cybercrime (art. 4 especially) and the draft of the Anti-Counterfeiting Trade Agreement.
[290] Proposal for a European Parliament and Council Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights, COM (2005) 276/1.

"necessary to ensure the effectiveness of Community law".[291] Read together with art. 207 of the TFEU, (which defines the "commercial aspects of intellectual property" as a part of the common commercial policy over which the EU regulators have legislative competence[292]), it could be seen as providing a legal basis for the harmonisation of criminal IP enforcement (which could subsequently be aimed at the IP infringers online).[293]

The Member States have refrained from committing themselves to such an interpretation. As Geiger notes in his paper from 2012, there are certain fundamental problems with the harmonisation of this branch of criminal enforcement.[294] Criminal law is a tool of the state which is supposed to be applied when the public interest is in danger – and the definition of "public interest" tends to differ between various Member States. Moreover, since criminal measures are potentially the strongest tools the state can employ in order to regulate its citizens' behaviour, the sovereignty issue comes into play as well.

Nevertheless, as foretold in the beginning of this section, some of the Member States established their own, national legal bases for making the relevant infringers criminally liable. The jurisdiction of England and Wales can serve here as an example, with the offence set by s. 107 of the CDPA 1998 as the primary incarnation of the discussed enforcement scheme (as applied in the area of copyright law). By virtue of this complex section, the principal mode of the statutory offence of criminal copyright infringement is committed if a person engages in one of the five activities with an article which he/she knows, or has reason to believe, to be an infringing copy of a copyrighted

[291] Case C-176/03 *Commission v Council*, at [52].
[292] TFEU, supra fn. 176, art. 207.
[293] Though for example Geiger pursues a different line of reasoning, stating that those provisions are conflicting, rather complementing each other – see Geiger C, 'The Anti-Counterfeiting Trade Agreement and Criminal Enforcement of Intellectual Property: What Consequences for the European Union?', in Rosen J (ed), IP Rights at the Crossroads of Trade (Edward Elgar 2012), at 6.
[294] Geiger, supra fn. 293, at 2.

work. Those activities are: making the infringing copy for sale or hire,[295] importing it into the UK otherwise than for this person's private and domestic use,[296] possessing it in the course of a business with a view to committing an act infringing the copyright attached to the copy,[297] doing one of the following with it in the course of a business[298] - selling or letting for hire,[299] offering or exposing for sale or hire,[300] exhibiting in public[301] or distributing,[302] and finally, distributing the copy otherwise than in the course of business, to such an extent that the distribution affects prejudicially the owner of the relevant copyright.[303]

Additionally, s. 107(2A) of the CDPA 1988 makes it an offence to infringe the copyright in a work by communicating this work to the public in the course of a business, or (if not in the course of a business) to such an extent that the copyright owner is prejudicially affected.[304]

In terms of sentencing, those found guilty of the offence set by s. 107 (1)(a), (b), (d)(iv) or (e), are liable to be imprisoned for up to 6 months and/or fined with the amount not exceeding 50,000 GBP (summary conviction), or imprisoned for up to 10 years and/or fined with an unlimited sum of money (conviction on indictment).[305] Those found guilty of the offence set by s. 107(2A) are liable to be imprisoned for up to 3 months and/or fined with the amount not exceeding 50,000 GBP (summary conviction), or imprisoned for up to 2 years and/or fined with an unlimited sum of money (conviction on indictment).[306]

---

[295] CDPA 1988, supra fn. 253, s. 107(1)(a).
[296] CDPA 1988, supra fn. 253, s. 107(1)(b).
[297] CDPA 1988, supra fn. 253, s. 107(1)(c).
[298] CDPA 1988, supra fn. 253, s. 107(1)(d).
[299] CDPA 1988, supra fn. 253, s. 107(1)(d)(i).
[300] CDPA 1988, supra fn. 253, s. 107(1)(d)(ii).
[301] CDPA 1988, supra fn. 253, s. 107(1)(d)(iii).
[302] CDPA 1988, supra fn. 253, s. 107(1)(d)(iv).
[303] CDPA 1988, supra fn. 253, s. 107(1)(e).
[304] CDPA 1988, supra fn. 253, s. 107(2A)
[305] CDPA 1988, supra fn. 253, s. 107(4).
[306] CDPA 1988, supra fn. 253, s. 107(4A).

One of the rather scarce instances of this section being used against a copyright-infringing filesharer is the case of a Scottish nurse from Ayr, who plead guilty to the charges made under s. 107(1)(e) of the CDPA (distributing the copy otherwise than in the course of business, to such an extent that the distribution affects prejudicially the owner of the relevant copyright).[307] Using an unspecified P2P network, the defendant made almost £54,000 worth of music files available to other users, for which activity she was sentenced to three years on probation and has been ordered to attend mandatory cognitive therapy treatment sessions for Obsessive Compulsive Disorder (the latter part of the sentence being given as a result of the defendant's personal mental health problems – copyright-infringing filesharing is not, at the time of writing, a condition requiring medical attention *per se*).[308][309]

In the trademarks area, there were certain occasions on which traders in counterfeit goods operating through eBay (their offers constituting a type of "infringing content" within the context of this thesis) became subject to criminal liability, much in the spirit of art. 61 of TRIPS.[310] In England and Wales, s. 92(1) of the Trademarks Act 1994 (hereafter referred to as TMA 1994) states that a person commits an offence if he "sells or lets for hire, offers or exposes for sale or hire or distributes goods which bear, or the packaging of which bears (…)"[311] a sign "(…) identical to, or likely to be mistaken for, a registered trade mark (…)"[312] – provided his actions were conducted "(…) with a view to gain for himself or another, or with intent to cause loss to another, and without the consent of the proprietor".[313] This offence was the main charge under which an online counterfeit trader was sentenced to prison

[307] See http://www.bbc.co.uk/news/uk-scotland-glasgow-west-13603003.
[308] See http://www.scotslawblog.com/criminal-law/ayr-woman-convicted-of-file-sharing-as-acs-law-gets-off-hook/.
[309] For similar cases, see also the Oink website users' case (http://torrentfreak.com/oink-uploaders-sentenced-to-community-service-090123/) and the US case of *Sony BMG v Tenenbaum* (2011) Nos. 10-1883, 10-1947, 10-2052, where a copyright-infringing filesharer was punished with a fine of $675,000.
[310] TRIPS, supra fn. 10, art. 61.
[311] Trademarks Act 1994 c. 26, s. 92(1)(b).
[312] Trademarks Act, supra fn. 311, s. 92(1)(a).
[313] Trademarks Act, supra fn. 311, s. 92(1).

for 21 months, after pleading guilty at Manchester's Minshull Street Crown Court.[314] The defendant was selling fake designer clothing on eBay, using almost thirty eBay usernames in order to cover up his tracks.[315]

As for the other two content types, that is privacy-infringing and defamatory content, the enforcement scheme based on imposing criminal liability on the infringer arguably holds much less presence. Nonetheless, there are some signs of this type of a legal response being relied on in the Member States' jurisdictions. For privacy-infringing content, an example can be provided by the revenge pornography-related offence set out in s. 33 of the UK's Criminal Justice and Courts Act 2015, which states that "it is an offence for a person to disclose a private sexual photograph or film if the disclosure is made (…) without the consent of an individual who appears in the photograph or film, and (…) with the intention of causing that individual distress". A corresponding example for defamatory content can be found within the defamation offences set out in the German Criminal Code.[316] For instance, the offence of defamation set under §186 states that:

- "Whosoever asserts or disseminates a fact related to another person which may defame him or negatively affect public opinion about him, shall, unless this fact can be proven to be true, be liable to imprisonment not exceeding one year or a fine and, if the offence was committed publicly or through the dissemination of written materials (section 11(3)), to imprisonment not exceeding two years or a fine".[317][318]

[314] See http://www.manchestereveningnews.co.uk/news/local-news/rogue-trader-who-made-1m-904645.
[315] See http://www.dailymail.co.uk/news/article-1336727/Ebay-conman-Amit-Sharma-34-weeps-hes-sent-prison.html.
[316] Orig. *Strafgesetzbuch* (StGB). Translation by Prof. Dr. Michael Bohlander available at http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1657.
[317] German Criminal Code, supra fn. 316, §186.
[318] The StGB contains further offences related to defamation, see §185 to §192.

2.3. Identifying the infringers.

This section of the chapter focuses on one particular challenge inherent to all enforcement schemes presented thus far – the identification of relevant online infringers. The issue of locating wrongdoers is also present in the offline world, but it gains a distinct dimension in cyberspace, due to the wide variety of ways in which users anonymise themselves. If all the rightholders have is, for example, the forum alias of the infringer going by the name of "XxIamSoAwesome69xX", they do not have much of a chance to impose civil or criminal liability on such a wrongdoer; and their options related to infringer-focused injunctive relief are limited as well. It should be added that while the very identification measures are oftentimes based around intermediary-oriented injunctions, the notion of identification is broad enough to be discussed in the following, separate section.

The challenge in question has long been recognised by the lawmakers on multiple levels, and they have in fact enacted certain regulatory instruments aimed at the identification of online wrongdoers, including those belonging to the areas of this thesis' interest. Starting with the international arena, we have art. 47 of the TRIPS Agreement, which states that:

- "Members may provide that the judicial authorities shall have the authority, unless this would be out of proportion to the seriousness of the infringement, to order the infringer to inform the right holder of the identity of third persons involved in the production and distribution of the infringing goods or services and of their channels of distribution".

Art. 47 presumes that the target of such an identification order would be an infringer himself, making it difficult to connect this provision to an identification order aimed at an online intermediary who did not incur civil or criminal liability for the infringing act. However, such a scenario was given

consideration by the European lawmakers. Art. 6(b) of the E-Commerce Directive obliges the ISPs to ensure that "the natural or legal person on whose behalf the communication is made" is clearly identifiable.[319] This is complemented by art. 15(2) of the same Directive, which declares that:

- "Member States may establish obligations for information society service providers (…) to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements".[320]

While the term "storage agreements" can be seen as slightly ambiguous, it seems most probable that it covers relationships typical for users of platforms such as cyberlockers, streaming websites, social media, blogs etc. It is worth adding here that in the realm of IP rights, the Enforcement Directive echoes art. 47 of TRIPS, by obliging the Member States to provide for ways of identifying the relevant infringer. In its article 8(1), the said Directive requires them to:

- "ensure that, in the context of proceedings concerning an infringement of an intellectual property right and in response to a justified and proportionate request of the claimant, the competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided by the infringer and/or any other person who:
    - (a) was found in possession of the infringing goods on a commercial scale;
    - (b) was found to be using the infringing services on a commercial scale;
    - (c) was found to be providing on a commercial scale services

[319] E-Commerce Directive, supra fn. 91, art 6(b).
[320] E-Commerce Directive, supra fn. 91, art. 15(2).

used in infringing activities; or

- (d) was indicated by the person referred to in point (a), (b) or (c) as being involved in the production, manufacture or distribution of the goods or the provision of the services".[321]

The CJEU had a chance to provide guidance with regards to such identification measures in the case of *Promusicae v Telefonica* (2008).[322] The referred case from Spain concerned an identification request made by the claimant to the defendant ISP, aimed at discovering the identities of filesharers using the Kazaa P2P network,[323] who allegedly infringed the claimant's copyright in a number of music files. ISPs are fairly often approached by the rightholders in such situations, for as Tsoutanis noted, they "know who is behind every IP-address they provide - or they at least have sufficient personal data to give proper leads to disclose the real identity of their customer: email addresses, bank accounts and telephone numbers, and often more".[324] The ISP in *Promusicae* refused to provide the demanded information, stating that according to the national law, "the data sought by Promusicae is authorised only in a criminal investigation or for the purpose of safeguarding public security and national defence, not in civil proceedings or as a preliminary measure relating to civil proceedings".[325]

The question referred to the CJEU was whether the relevant instruments of the EU law[326] allow the Member States to limit the availability of the identification requests at hand to instances submitted by the defendant.[327] The Court responded that the relevant provisions of the EU law "do not require the Member States to lay down, in a situation such as that in the main

[321] Enforcement Directive, supra fn. 247, art. 8(1).
[322] Case C-275/06 *Promusicae v Telefonica*.
[323] Which functions in a similar manner to the Grokster P2P network, discussed in chapter one, section 2.2.3.3.
[324] Tsoutanis A, 'Privacy and piracy in cyberspace: justice for all'(2014) Journal of Intellectual Property Law & Practice 8(12), at 953.
[325] *Promusicae v Telefonica*, supra fn. 322, at [33].
[326] Primarily the E-Commerce Directive, the InfoSoc Directive, the Enforcement Directive and the Data Protection Directive – *Promusicae v Telefonica*, supra fn. 322, [6] to [26].
[327] *Promusicae v Telefonica*, supra fn. 322, at [34].

proceedings, an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings".[328] However, it added right away that the Member States must interpret the relevant Directives in a manner which strikes a fair balance between various fundamental rights protected by the Community law[329] - what, in essence, means that the Member States have the *option* of placing such identification-focused obligations, if they see them as essential to the protection of interests such as, for example, intellectual property, privacy and reputation of their citizens.

2.4. Graduated response schemes.

Having discussed the challenge of identifying the infringers for the purpose of civil and criminal proceedings, we can proceed to the next, relatively novel enforcement scheme, which became known as the "graduated response" or the "three-strikes" approach. In contrast to the schemes presented above, this avenue of online enforcement has so far gained actual presence only in the area of copyright-infringing P2P filesharing.

The graduated response approach bears some resemblance to the earlier mentioned litigation schemes[330] - with arguably more organisation and a greater focus on deterrence. The core of this enforcement scheme is as follows: the infringing P2P users are located with the help of their ISPs, but instead of being subjected to any form of liability or a court injunction straight away, they have a chance to cease their illicit activity by themselves – for after a certain number of times they are caught, they might end up getting punished; for example, by being taken to court or by being subjected to measures limiting their Internet connection.

[328] *Promusicae v Telefonica*, supra fn. 322, at [70].
[329] *Promusicae v Telefonica*, supra fn. 322, at [70].
[330] Covered in section 2.1 of the current chapter.

The reason why this kind of an enforcement scheme is included in this thesis is twofold; first of all, there is the previously mentioned presumption of deterrence. If the infringing users cease their activities due to the received warnings/infringement reports (or due to the consequent, more punitive measures), they are no longer making the infringing material available, and thus the access to such content is removed. Secondly, limiting the notorious infringer's connection might (in theory) distance him from the infrastructure required for his illicit activities.

The most notable aspects of the graduated response approach appeared in France (via the so-called HADOPI law[331]), UK (via the Digital Economy Act 2010,[332] hereafter referred to as the DEA 2010) and US (via a voluntary[333] agreement between the US copyrightholders and ISPs, known as the Copyright Alert System or "the six-strikes" plan[334]). The following section uses the British Act as an example demonstrating the inner workings of a graduated response-type enforcement scheme.

The DEA 2010 introduced two key procedures aimed at reducing online piracy – labelled as the "initial obligations" and the "obligations to limit Internet access". The first procedure starts with a copyright owner accessing one of the P2P filesharing networks, and attempting to find and download a file to which he owns the copyright. Once he succeeds, he is supposed to record the IP address of the user who made the copyrighted file available, and send it to this user's ISP in the form of a Copyright Infringement Report (CIR). By virtue of s. 3 of the Act, the ISP is then required to forward this CIR to the allegedly infringing user.[335] Should a user receive more than three CIRs, each of them separated from another by a specific period of time, he is put on this

[331] Loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet (HADOPI Law).
[332] Digital Economy Act 2010 c. 24.
[333] This word should probably not be taken too literally.
[334] See http://www.copyrightinformation.org/the-copyright-alert-system/.
[335] DEA 2010, supra fn. 332, s. 3.

ISP's "copyright infringement list".[336] By virtue of s. 4, the copyright owner may demand the ISP to provide him with an anonymous list of all users who reached the threshold by infringing his copyright.[337] Upon receiving the list, the copyright owner may then apply for a court injunction to identify the infringing users and commence infringement proceedings against them.[338]

The second procedure, known as the "obligations to limit Internet access", is to be implemented only if the Secretary of State decides that the initial obligations regime does not perform sufficiently well in reducing online piracy, after at least a year of operation.[339] This second procedure would impose an obligation on the ISPs to affect the Internet connection of its subscribers who reached the threshold of CIRs or went above it. This could potentially include measures such as limiting the speed of the connection, preventing the subscriber from accessing certain online services, and in the ultimate case, suspending the subscriber's connection altogether.[340]

However, none of those procedures has (at the time of writing) been actually implemented. After a series of setbacks, the UK government announced that the initial obligations regime was to be activated in the second half of 2015[341] - but in March 2016, there is still no sign of it. It is difficult to avoid the impression that the British government abandoned pushing this enforcement scheme forward, especially given the appearance of a voluntary agreement akin to that which was signed in the US. It is known as Creative Content UK, and it was signed in 2014[342] - in essence, it is the initial obligations regime from DEA 2010, focused only on notifications to the users, devoid of the

[336] DEA 2010, supra fn. 332, s. 3.
[337] DEA 2010, supra fn. 332, s. 4.
[338] DEA 2010, supra fn. 332, s. 4.
[339] DEA 2010, supra fn. 332, s. 9 and 10.
[340] While the Act itself does not specify those measures, the Digital Britain Report (2009), published by DCMS & BIS, suggests them at page 111.
[341] See http://www.bbc.co.uk/news/technology-22796723.
[342] See http://www.bbc.com/news/technology-28374457

threat of the user's data being transferred to the rightholders. It is hoped that this purely educational measure is going to deter the infringers nevertheless.[343]

On the French side of things, the enthusiasm for the graduated response approach seems to be dwindling as well. While the HADOPI law was the first legislative project to endorse the discussed measures, the French government gradually moved away from the three-strikes scheme; for example, in July 2013, the technical measures (such as the suspension of the Internet connection) of the scheme were parted with.[344] While we have yet to see how the US take[345] on the graduated response approach fares, it seems that this new type of an enforcement scheme is having difficulties with becoming a firmly established anti-online piracy measure.

2.5. Digital Rights Management.

The last enforcement scheme presented in the infringer-focused part of chapter two is the use of various forms of Digital Rights Management (hereafter referred to as DRM and DRMs). This term denotes the practice of implementing technological measures designed to limit the user's control over a digital product. Following on the overarching topic of this thesis, this section focuses on the DRM schemes aimed at preventing the infringement of the relevant legitimate interests; well, one of them, to be more specific. Similarly to the graduated response approach, DRMs have so far been only implemented within the area of copyright law. The conceptual underpinning of this enforcement scheme (in the discussed context) is as follows: if rightholders release their content with safeguards preventing, for example, the unauthorised copying/sharing of the work in cyberspace, certain avenues of access to infringing material might become closed.

[343] For further discussion of the deterrence effect, see section 3.1 of chapter three.
[344] See http://www.pcinpact.com/news/80487-hadopi-600-d-amende-et-quinze-jours-suspension-pour-abonne.htm.
[345] Supra fn. 334.

It is possible to draw a distinction between two types of DRM measures; the Technological Protection Measures (hereafter referred to as TPMs) and Rights Management Information measures (hereafter referred to as RMIs). The latter category focuses on the remote control of access to the "host" information, while the former is more concerned with restricting the unauthorised copying of the said information.[346] Examples of both TPMs and RMIs are presented in the following paragraph.

The anti-copying measures on CDs and DVDs (containing, for example, copyrighted music, videos, software and video games) are a classic representation of a TPM scheme. Another, slightly more sophisticated, example from this category of DRMs could be the use of "text watermarks" in copyrighted eBooks, allowing the rightholders to trace the person who performed the initial act of unauthorised reproduction.[347] As for the RMIs, the realm of video gaming provides us with two interesting examples. Firstly, many online games nowadays require a subscription – although the user has the game installed on his hard drive, the in-built RMI will not allow him to play the game without paying his monthly fee.[348] Secondly, certain game developers started to require their customers to be online in order to enjoy the game; example being Blizzard with their 2012 title, Diablo 3.[349] This allows for the continuous verification of the user's version of the game and grants persistent control over its content (via, for example, mandatory updates). That being said, the TPMs are arguably of greater relevance to this thesis, since they are closer to the goal of removing access to infringing content – RMIs are usually focused on the user's interaction with the legitimate copy of the copyrighted work. Finally, it has to be remembered that this is very much an

[346] For example, see MacQueen H, 'Appropriate for the digital age'? Copyright and the Internet: 2. Exceptions and Licensing', in Edwards L and Waelde C (eds) Law and the Internet, 3rd ed. (Hart Publishing 2009), at 217.
[347] See https://torrentfreak.com/new-drm-changes-text-of-ebooks-to-catch-pirates-130616/.
[348] The most visible example here would be MMO games, such as World of Warcraft, EVE Online or The Secret World.
[349] See http://www.pcgamer.com/2012/07/19/diablo-3-always-online-requirement-critical-to-d3s-long-term-integrity-says-blizzard-boss/.

inconclusive list of existing DRMs, for this type of an enforcement measure can be tailored to suit various categories of copyrighted works, on an individual manner.

Through the Information Society Directive, DRMs aimed at preventing the infringement of copyrighted works have been given legal protection on the European level. Art. 6(1) of this Directive provides that: "Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective".[350] Art. 6(2) goes on to specify the situations in which such protection is required,[351] with art. 6(3) defining technological measures as "any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject matter, which are not authorised by the rightholder".[352] Moreover, RMIs are granted similar, express protection by art. 7 of the InfoSoc Directive.[353]

In this context, it is worth mentioning a case originating from the US, which dealt with a particular "link" in the chain of copyright-infringing filesharing, focused on removing DRMs from copyrighted works. In *Griffiths v United States of America* (2005),[354] the accused was a member of one of the so called release/warez groups, activities of which focus on breaking DRMs on copyrighted files and releasing them to the public (hence, the term "release group"). The defendant was charged in the US with criminal copyright infringement, as well as conspiracy-related offences, and (what was the key motion in the referred case) extradited from Australia to the US.[355]

[350] Information Society Directive, supra fn. 8, art. 6(1).
[351] Information Society Directive, supra fn. 8, art. 6(2).
[352] Information Society Directive, supra fn. 8, art. 6(3).
[353] Information Society Directive, supra fn. 8, art. 7.
[354] *Griffiths v United States of America* [2005] FCAFC 34.
[355] What provides an interesting point for section 2.2, focused on criminal liability – it shows that measures as severe as extradition can be used against the (copyright) infringers.

3. Enforcement schemes focused on the intermediary.

As time passed, the rightholders started to notice that dedicating their resources to enforcement efforts aimed solely at the infringer might not be the best response to the problem of online content infringing their rights. As Eziefula noted in the context of P2P copyright-infringing content, the creative industries realised that the infringer-orientated "litigation alone would not solve the problem, even if supported with educational initiatives and attractively priced legal music services".[356] A similar line of reasoning comes from Davies, who submitted that "[i]t seems insufficient today for those holding intellectual property rights to seek redress against "primary infringers" alone".[357] The perceived insufficiency of this approach most likely arose primarily due to the concerns over its effectiveness,[358] as well as due to its inherent challenges, such as the problem of identifying the infringer.[359] While the cited academic commentators expressed their position in relation to copyright-infringing content, it seems plausible to conclude that a similar dissatisfaction with the purely infringer-focused approach could be found amongst the other rightholders, whose trademarks, privacy or reputation was/were infringed by means of online content.

Consequently, the rightholders (and governments) turned their attention towards the online intermediaries, whose services are used to facilitate the spread of the infringing content. The Digital Music Report prepared by the International Federation of the Phonographic Industry (hereafter referred to as

[356] Eziefula N, 'Getting in on the Act - OfCom publishes draft code on Digital Economy Act initial obligations' (2010) Ent. L.R. 21(7), 253, at 253.
[357] Davies P 'Accessory liability: protecting intellectual property rights' (2011) I.P.Q. 4, 390, at 390.
[358] See chapter three.
[359] See section 2.3 of the current chapter. Of course, the difficulties tied to the identification of infringers are, among others, one of the elements making for the problems with the effectiveness of the infringer focused approach.

the IFPI) stated that such intermediaries are "uniquely situated"[360] to help in tackling the problem of pirated copyrighted works – and, one could propose, other types of infringing content as well. Edwards probably put it more accurately, when she wrote that ISPs (and, it could be added, many other intermediaries) "hold an unfortunate piggy-in-the-middle position".[361] Then again, this position is probably also that of the lowest cost avoider. However one wishes to see it, there is little doubt that the outlined development in the area of online enforcement policy resulted in the creation of a wide array of intermediary-focused enforcement schemes, oftentimes outmatching their infringer-focused counterparts in terms of legal complexity. Hence, this subchapter tries to present a map of the labyrinth created by the development of the enforcement schemes focused on multiple intermediaries.

In terms of structure, the first two sections of this part of the thesis mirror its predecessor, covering the approaches based on civil (section 3.1) and criminal (section 3.2) liability of the intermediaries. The complementary section 3.3 focuses on the principal legal constructs through which the liability of intermediaries is limited within the European Union's legal framework.

3.1. Subjecting the intermediaries to civil liability.

3.1.1. Modes of intermediary liability.

The following section aims to present a selection of civil liability doctrines which have been relied on within the EU by the four categories of rightholders, whose legitimate interests (copyright, trademark, privacy or reputation) were infringed through the use of the defendant intermediaries' online services. The said modes are a prerequisite of the award of damages, as

[360] *Digital Music Report: Expanding Choice. Going Global* (2012) by IFPI, at 17.
[361] Edwards L, 'Mandy and Me: Some Thoughts on the Digital Economy Bill' (2009) SCRIPTed 6(3), 535, at 537.

well as, depending on the case, of the intermediary-oriented injunctions, which (due their vast variety) are covered separately, in section 3.1.2 of this chapter. While grounds of infringer liability were discussed in chapter one, the modes of intermediary liability deserve to be discussed in this chapter in-depth; and as it might be predictable by now, particular attention is given to the modes of liability originating from England and Wales.

There are two things which should be underlined here upfront. First of all, the aim of this section is not to provide a detailed, complete overview of all types of civil liability imposed within the EU on the relevant intermediaries – its main concern is showing that such an approach to online enforcement exists, and presenting examples of routes leading to its application. Secondly, this section has to be read in conjunction with section 3.4 of this chapter, which covers limitations on the liability of intermediaries (most significantly, those set out in the E-Commerce Directive[362]), for as Kulk and Zuiderveen rightly noted in the context of copyright – "the rules governing the liability of internet intermediaries for copyright infringement are a patchwork of European Directives, national implementing legislation and different national liability regimes".[363] And as it will be shown, this "patchwork" analogy extends beyond the area of copyright.

3.1.1.1. Joint tort liability.

This mode of civil liability, present in the jurisdiction of England and Wales,[364] comes into play whenever two or more parties become liable for a single tortious loss suffered by the claimant; with the said loss having been caused by - for example - the infringement of claimant's copyright, trademark, privacy or reputation. However, it is crucial for those parties to have acted in a certain form of agreement, as demonstrated by the words of Lord Templeman

[362] E-Commerce Directive, supra fn. 91.
[363] Kulk S and Zuiderveen F, 'Filtering for copyright enforcement in Europe after the Sabam cases' (2012) E.I.P.R. 34(11) 791, at 792.
[364] (But not exclusive to it.)

in the case of *CBS v Amstrad* (1988);[365] "joint infringers are two or more persons who act in concert with one another pursuant to a common design in the infringement".[366]

The term "common design" has proven to be quite an interpretative challenge for the English courts. Since it is a crucial element of joint tort liability, it is worth taking a closer look at the extracts of judicial decisions which attempted to clarify its meaning, after which this section is going to move onto the examples showing the application of joint tort liability in relevant online scenarios.

In the earlier mentioned copyright case of *CBS v Amstrad*, the secondary defendant's[367] conduct identified as "procurement" was stated to be the key element leading to the finding of the common design. In an effort to characterise the behaviour constituting procurement of the primary defendant's infringement, Lord Templeman stated that modes of procurement, such as "inducement, incitement, or persuasion"[368] have to be conducted "by a defendant to an individual infringer and must identifiably procure a particular infringement in order to make the defendant liable as a joint infringer".[369]

The scope of the factual scenarios falling under the term "common design" was arguably widened in the case of *Unilever v Gillette* (1989),[370] where Mustill LJ submitted a broader interpretation of this concept, stating that it "(…) does not, as it seems to me, call for any finding that the secondary party has explicitly mapped out a plan with the primary offender. Their tacit agreement will be sufficient".[371] Moreover, he also submitted that there is actually no "need for a common design to infringe. It is enough that the parties

[365] *CBS Songs Ltd v Amstrad Consumer Electronics Plc* [1988] A.C. 1013.
[366] *CBS Songs v Amstrad*, supra fn. 365, at 1057.
[367] This being the one who facilitated the primary defendant's act of infringement.
[368] *CBS Songs v Amstrad*, supra fn. 365, at 1058.
[369] *CBS Songs v Amstrad*, supra fn. 365, at 1058.
[370] [1989] R.P.C. 583.
[371] *Unilever v Gillette*, supra fn. 370, at 609.

combine to secure the doing of acts which in the event prove to be infringements".[372]

The picture is further enriched by the decision in *Sabaf SpA v MFI Furniture Centres Ltd* (2002),[373] which attempted to explain the core of joint tort liability by putting emphasis on the idea of making the primary tortious act "one's own"., while maintaining the use of the term "common design". The relevant passage of the judgment proclaimed that:

- "The underlying concept for joint tortfeasance must be that the joint tortfeasor has been so involved in the commission of the tort as to make himself liable for the tort. Unless he has *made the infringing act his own*, he has not himself committed the tort. That notion seems to us what underlies all the decisions to which we were referred. *If there is a common design or concerted action or otherwise a combination to secure the doing of the infringing acts, then each of the combiners has made the act his own and will be liable*".[374]

Let us now turn towards the instances in which online intermediaries - whose services were used by the primary tortfeasors to infringe the relevant legitimate interests - were faced with claims aimed at making them jointly liable with the primary infringers. To this end, this section presents and compares two cases, mentioned in the first chapter; *L'Oréal v eBay* (though this time, we are concerned with its UK limb)[375] and *Fox v Newzbin*.[376]

The factual background of the trademark case of *L'Oréal v eBay* can be found above, in section 3.2 of chapter one – hence, the claim of joint tort liability

[372] *Unilever v Gillette*, supra fn. 370, at 609.
[373] [2003] R.P.C. 14.
[374] *Sabaf SpA v MFI*, supra fn. 373, at [59], emphasis added.
[375] [2009] EWHC 1094 (Ch).
[376] *Fox v Newzbin*, supra fn. 122.

against the online auction website can be considered straight away. Initially, Arnold J identified three factors which could be indicating that the operators of eBay were jointly liable for trademark infringements of the platform's users, stating that the former:

- "(…) do *facilitate* the infringement of third parties' trade marks, including L'Oréal's Trade Marks, by sellers; they do *know* that such infringements have occurred and are likely to continue to occur; and they *profit* from such infringements except where the rights owner makes a VeRO complaint[377] in sufficient time".[378]

However, the judge stated immediately after that "these factors are not enough to make eBay Europe liable as joint tortfeasors (…)" for "it cannot be said that the facility is one which inherently leads to infringement. It is capable of being used by sellers in a manner which does not infringe third party trade marks".[379] He concluded by declaring that since "(i) eBay Europe is under no legal duty to prevent infringement and (ii) facilitation with knowledge and an intention to profit is not enough",[380] the website's conduct does not put it within the reach of joint tort liability.

In his article from 2012 following *L'Oréal v eBay*, Lievens commented that "in the US and England, for example, eBay has been enjoying nothing but a tropical legal climate due to trade mark owners being confronted with overly burdensome joint tort liability standards".[381] According to him, the case at hand contributed to this situation by further narrowing down of the *Unilever* test for joint tort liability with additional criteria, thus providing that an online auction website such eBay would be liable only if it had "actively encouraged, favoured or knowingly facilitated a counterfeit seller in committing

[377] A VeRO complaint is a complaint made through eBay's N&T scheme.
[378] *L'Oréal v eBay* (UK), supra fn. 375, at [381], emphasis added.
[379] *L'Oréal v eBay* (UK), supra fn. 375, at [382].
[380] *L'Oréal v eBay* (UK), supra fn. 375, at [382].
[381] Lievens D, 'L'Oréal v. eBay - welcomed in France, resented in England.' (2012) IIC 43(1) 68, at 68.

infringements and the facilities which it provided had inherently led to those infringements".[382] One would be inclined to agree with the writer in question when he says that in practice, *L'Oréal v eBay* moves very close to demanding the proof of an online auction website's intention to infringe the claimant's trademark.[383]

Let us now turn towards *Fox v Newzbin*. While the judge in third decision referred to *L'Oréal v eBay*, he found the facts of the Usenet indexing service case to be leading to a different outcome – Newzbin was found to have acted in common design with the infringers (the premium members, specifically), and hence, to be jointly liable with them. Kitchin J declared that:

- "(…) the defendant well *knows* that it is making available to its premium members infringing copies of films, including the films of the claimants. In summary, the defendant operates a site which is *designed and intended to* make infringing copies of films readily available to its premium members; the site is structured in such a way as to promote such infringement by guiding the premium members to infringing copies of their choice and then providing them with the means to download those infringing copies by using the NZB facility".[384]

Furthermore, it was added that Newzbin's operators "encouraged and induced"[385] the website's editors to index copyright-infringing movie files (including those belonging to Fox), as well as gave their premium members advice about the procedures related to infringing filesharing, through dedicated forums.[386]

[382] Lievens, supra fn. 381, at 72.
[383] Lievens, supra fn. 381, at 72.
[384] *Fox v Newzbin*, supra fn. 122, at [111], emphasis added.
[385] *Fox v Newzbin*, supra fn. 122, at [111].
[386] *Fox v Newzbin*, supra fn. 122, at [111].

What then makes an online intermediary (whose service is used for infringing purposes) jointly liable in tort under the English law? Part of the answer to this question might be obtained by looking at the two cases described above together – while one of them dealt with copyright and the other with trademarks, the similar position of the defendants allows for such a comparison.

First of all, let us consider the similarities. In both cases, the online intermediaries were found to facilitate the infringements, possess the knowledge of this fact, as well as profit from it. The crucial factor which made the difference was whether the defendants' services inherently lead to infringement/were designed for infringing purposes. In *L'Oréal* this was held not to be the case, with Arnold J stating that "systems and policies neither favoured nor encouraged the listing or sale of counterfeit goods", while in *Newzbin*, Kitchin J presented a long list of factors indicating the opposite outcome. The validity of some of those factors is rather questionable – for example, "guiding the premium members to infringing copies of their choice and then providing them with the means to download those infringing copies by using the NZB facility" does not constitute a website's design feature; at its core the website guided the premium members to files shared through Usenet, be they infringing or not, and as far as this matter of design comes, Newzbin is no different from eBay. Nevertheless, the evidence demonstrating the operators' activities specifically tied to infringing content (such as guiding the editors towards pirated movies and giving infringement-related forum advice) seems to be a solid basis for the finding of common design to infringe.

Therefore, one has to wonder whether online intermediaries who are not found to have treated legitimate and infringing content differently can be held jointly liable for the infringements of their users. The significance of the online service's legitimate use might be playing here a strong, yet indirect role; eBay is primarily a website used for considerable legitimate purposes, Newzbin was

definitely not – this could have lead Kitchin J to include the earlier mentioned, potentially questionable factors.

As Llewelyn wrote, "although many cases have dealt with "common design" as a cause of action, the cases remain incoherent and in many ways inconsistent".[387] Joint tort liability can be used to impose civil liability on the relevant online intermediaries – but it might become quite a challenge for the claimants to prove it, especially where there is no evidence of the defendant's activity tied to infringing content specifically.

3.1.1.2. Authorisation liability.

The case of *Newzbin* appears again in this part of the thesis, by providing an example of an instance where an online intermediary was subjected to authorisation liability resulting from the infringing acts of its users. As in section 3.2.1, it is worth providing some background on this mode of liability before discussing its application to cases involving the earlier mentioned intermediaries.

In the context of UK copyright law, section 16(2) of the CDPA 1988 provides that "copyright in a work is infringed by a person who without the licence of the copyright owner does, or *authorises* another to do, any of the acts restricted by the copyright".[388] That being said, the concept of authorisation liability has been present in the UK law for quite a while and it predates the CDPA 1988. Hence, before heading back to *Newzbin*, it is worth looking at how this concept was interpreted in two key UK cases.

[387] Llewelyn D, 'Intellectual property liability of consumers, facilitators and intermediaries: Concepts under Common Law', in Heath C and Sanders A (eds), Intellectual property liability of consumers, facilitators and intermediaries (2012), at 26.
[388] CDPA 1988, supra fn. 253, art. 16(2), emphasis added.

First of all, the copyright case of *Falcon v Famous Players Film Co* (1926)[389] stated that "to 'authorise' means to grant or purport to grant to a third person the right to do the act complained of, whether the intention is that the grantee shall do the act on his own account, or only on account of the grantor;(…)."[390] Secondly, there is the earlier mentioned House of Lords' judgment in *CBS v Amstrad* (1988).[391] Since the facts of this case provide for an interesting comparison with the cases of online intermediaries discussed in this thesis, it is worth to briefly summarise them here. The defendant was a manufacturer and seller of hi-fi equipment which allowed its users to copy music from one tape to another. The claimant, representing the music industry, submitted that by selling such a device, the defendants authorised and incited the infringement of claimant's copyrighted works. While the Court stated that the grant of authority can be either express or implied,[392] it dismissed the submitted claim, finding the defendant's conduct to be that of a legitimate company. In justifying this verdict, Lord Templeman dismissed the proposed reasoning found in Laddie, Prescott and Vitoria's *Modern Law of Copyright*, which stated that;

- "a person may be said to authorise another to commit an infringement if the one has some form of control over the other at the time of infringement or, if he has no such control, is responsible for placing in the other's hands materials which by their nature are almost inevitably to be used for the purpose of infringement".[393]

According to the law lord, such a position would be too wide; instead, he adopted the reasoning accepted in the earlier case of *CBS v Ames Records & Tapes Ltd* (1981),[394] stating that "an act is not authorised by somebody who merely enables or possibly assists or even encourages another to do that act,

[389] [1926] 2 K.B. 474.
[390] *Falcon v Famous Players Film*, supra fn. 389, at 499.
[391] *CBS v Amstrad*, supra fn. 365.
[392] *CBS v Amstrad*, supra fn. 365, at 1053-1055.
[393] Laddie H, Prescott P & Vitoria M, *The Modern Law of Copyright* (Butterworths 1980), at 403.
[394] [1981] 2 All E.R. 812.

but does not purport to have any authority which he can grant to justify the doing of the act".[395]

In *Newzbin*, Kitchin J stated accordingly that on the basis of the judgment in *Amstrad*, "it is clear (…) that "authorise" means the grant or purported grant of the right to do the act complained of. It does not extend to mere enablement, assistance or even encouragement".[396] Nevertheless, he found the conduct of the operators of the Usenet-indexing website to fall under authorisation liability. In doing so, Kitchin J brought attention to several factors. First of all, he established that a close relationship existed between the operators and the website's premium users, due to the former's provision of sophisticated filesharing facilities to the latter.[397] Secondly, the operators' activity was regarded as going beyond content-neutral indexing and categorisation, for it included, for example, tagging and providing the description of the indexed content.[398] Thirdly, the judge stated that it was clear from the "movies" tab on the website that there is a lot of infringing content being shared through Newzbin, and yet its operators did not undertake any preventive steps (such as installing a filtering scheme) to fix this situation.[399] Additionally, it is worth adding that the defendant's argument about the contractual restrictions placed on editors and website users (preventing them from committing copyright infringing acts) was dismissed by the judge as being merely a "window dressing", such restrictions being contradicted by the way in which the defendants operated their website. On the basis of those factors, Kitchin J concluded that;

- "a reasonable member would deduce from the defendant's activities that it *purports to possess the authority* to grant any required permission to copy any film that a member may choose from the Movies category on Newzbin and that the defendant has sanctioned,

[395] *CBS v Ames Records*, supra fn. 394, at 106.
[396] *Fox v Newzbin*, supra fn. 122, at 90.
[397] *Fox v Newzbin*, supra fn. 122, at 98.
[398] *Fox v Newzbin*, supra fn. 122, at 99.
[399] *Fox v Newzbin*, supra fn. 122, at 101.

approved and countenanced the copying of the claimants' films".[400]

It is perhaps slightly difficult to reconcile this part of the *Newzbin* decision with the reasoning endorsed in *CBS v Amstrad*. While Lord Templeman stressed that merely enabling, assisting or even encouraging does not give rise to authorisation of liability (unless the defendant purported to possess the authority mandating the infringing activity), Kitchin J seemed to, at times, rely on such factors in the process of establishing that Newzbin's operators "purported to possess" the relevant authority. Indexing and tagging of content, or being aware of the infringing activities occurring on Newzbin sounds more like "merely enabling" or (if one wish to see it so) "encouraging" the infringing activity, rather than pretending to have some kind of authority warranting its presence.

Following *Newzbin*, the copyrightholders wishing to act against the online intermediaries facilitating the infringement of their works might wish to rely on authorisation liability more often. That being said, the concept of "authorisation" continues to be a rather elusive one – and while in *Newzbin* the information leading to the infringing content was indexed by the website's operators/contracted editors, it is uncertain how authorisation liability would be applied to intermediaries whose services also facilitate copyright-infringing filesharing, but where the infringing content/indexing information on such services is either provided by the users or generated by much more automatic means. Overall, it seems plausible to agree with Savola's critical opinion of the use of authorisation liability in the discussed context - "given that users are responsible for their own activities, it is submitted that a purported grant to infringe should require significantly more and for clarity something explicit rather than mere provision of a website well suited for infringement".[401]

3.1.1.3. Liability for communication to the public.

[400] *Fox v Newzbin*, supra fn. 122, at 102.
[401] Savola P, 'Blocking injunctions and website operators' liability for copyright infringement for user-generated links' (2014) E.I.P.R. 2014, 36(5), at 285.

In the context of this thesis, joint tort liability and authorisation liability seem to be specifically focused on allocating "secondary" liability to online intermediaries with regards to the specific role such intermediaries play in facilitating, enabling, etc. of the primary infringer's conduct. As it will be shown, the third mode of liability discussed in this section - the liability for communication to the public - seems to be moving conceptually closer towards treating online intermediaries as primary infringers. Since this is the third mode of civil liability under which the operators of Newzbin were found to be liable for the acts of their users, it is worth covering it here as well.

Within UK copyright law, the legal basis for making online intermediaries liable for communication to the public is the same as the one employed against the copyright-infringing users – namely, section 16(1)(d) of the CDPA 1988 (implementing art. 3 of the Infosoc Directive[402]), which states that the copyrightholders in the UK have the exclusive right to communicate their works to the public.[403]

Using the CJEU *Rafael Hoteles* (2006)[404] case as the point of reference, Kitchin J found the operators of Newzbin to be liable for communicating the claimants' works to the public. The key factors which led him to this finding were that "… the defendant has intervened in a highly material way to make the claimants' films available to a new audience (…)",[405] that there is "(…) no doubt that the defendant's premium members consider that Newzbin is making available to them the films in the Newzbin index",[406] and that the defendant "provided its service in full knowledge of the consequences of its actions".[407]

---

[402] Which is discussed in chapter one, section 2.1.2.
[403] CDPA 1988, supra fn. 253, s. 16(1)(d).
[404] Case C-306/05 *Sociedad General de Autores y Editores de Espana (SGAE) v Rafael Hoteles SL* [2006].
[405] *Fox v Newzbin*, supra fn. 122, at 125.
[406] *Fox v Newzbin*, supra fn. 122, at 125.
[407] *Fox v Newzbin*, supra fn. 122, at 125.

It is worth adding that liability for communication to the public was also used in a line of cases following the *Fox v BT* judgment, as a basis for the award of site-blocking injunctions. This includes the earlier mentioned[408] judgments in *Dramatico Entertainment v British Sky Broadcasting (No. 2)*,[409] *EMI Records Ltd v British Sky Broadcasting Ltd*,[410] and *Football Association Premier League Ltd v British Sky Broadcasting Ltd & Others*,[411] as well as, for a further example, the later decision in *Paramount Home Entertainment International Ltd v British Sky Broad-casting Ltd* (2013).[412] In the last case, the site-blocking injunctions were granted on the similar legal basis against two streaming websites, SolarMovie and TubePlus.

Looking back to the question of whether certain modes of liability (for example, authorisation liability) would be successfully applied against online intermediaries who have a less active role than Newzbin did in the delivery of infringing content (or indexing information corresponding to it), it seems that as far as communication to the public goes, such a question is being answered affirmatively by the UK courts. That being said, it has to be underlined that so far, authorisation liability and liability for communication to the public are tied to copyright-infringing content – at the time being, they do not apply to the other three types of infringing content.

3.1.1.4. Publisher's liability.

Section 3.1.1.2 of the current chapter has demonstrated how (as it often happens) a seemingly clear word from the common language – authorisation – might gain a whole new dimension of complexity upon being incorporated into the legal language. Publisher's liability, which this section focuses on, serves as an another example of this kind, and portrays well the situation in

[408] See section 2.2.3.1. of chapter one.
[409] Supra fn. 117.
[410] Supra fn. 119.
[411] Supra fn. 526.
[412] [2013] EWHC 3479 (Ch).

which a legal concept might change in the online setting, as noted by Reed in the context of publisher's liability in defamation cases.[413]

Remaining in this content area, this section is going to start by considering instances where defamed claimants sought to impose publisher's liability on online intermediaries whose services were used to spread the defamatory content. This is due to the fact that the concept of a publisher is vital to liability in the UK law of defamation,[414] as opposed to the law of copyright, which is discussed in the latter part of this section.

The first case which deserves to be presented here is the earlier mentioned *Godfrey v Demon Internet* (2001).[415] There, the defendant ISP was held liable for the defamatory posts published on a Usenet newsgroup hosted by the said ISP. It was established that as soon as an online service provider becomes aware (ie. acquires actual knowledge) of the defamatory use of its service, it becomes liable in common law as a publisher of the defamatory information. Then, it has to remove the said infringing content expeditiously, in order to prevent the further dissemination of the defamatory material – or become liable in damages to the claimant.[416]

The case involved an interpretation of the so-called innocent dissemination defence, which is worth being covered in more detail. The defence, currently laid out in s. 1(1) of the Defamation Act 1996, states that "(i)n defamation proceedings a person has a defence if he shows that he was not the author, editor or publisher of the statement complained of,[417] he took reasonable care in relation to its publication,[418] and he did not know, and had no reason to believe, that what he did caused or contributed to the publication of a

[413] Reed C, 'Information "Ownership" in the Cloud' (2010) Queen Mary School of Law Legal Studies Research Paper No. 45/2010, available at (http://ssrn.com/abstract=1562461), at 250.
[414] See chapter one, section 5.1.
[415] *Godfrey v Demon Internet*, supra fn. 229.
[416] *Godfrey v Demon Internet*, supra fn. 229, at 206.
[417] Defamation Act 1996 c. 31, s. 1(1)(a)
[418] Defamation Act, supra note 417, s. 1(1)(b)

defamatory statement.[419]" A "publisher" is defined in the Act as a "commercial publisher, that is, a person whose business is issuing material to the public, or a section of the public, who issues material containing the statement in the course of that business."[420] However, importantly for online intermediaries, this term does not encompass an entity whose only involvement in the publication is "as the operator of or provider of access to a communications system by means of which the statement is transmitted, or made available, by a person over whom he has no effective control."[421] In *Godfrey*, while the ISP was not the author, editor or commercial publisher of the statement, it failed to show both that it took reasonable care in relation to the defamatory posting, and that it did not have actual or constructive knowledge that its actions lead to the defamatory publication.[422]

Three different ISPs (AOL, Tiscali and BT) found themselves at the crosshair of publisher's liability for defamatory statements in a latter case of *Bunt v Tilley* (2007).[423] The difference was that they were not hosting, for example, a newsgroup where defamatory posts could appear – they were sued for the mere provision of the Internet connection which was used by their subscribers to post defamatory messages on third party websites. However, the court found that the three ISPs cannot be regarded as publishers of the defamatory statements – instead, they should be seen as passive facilitators, lying outside of the scope of publisher's liability. The key factor which might bring an online intermediary within the role of a publisher was characterised by Eady J as "knowing involvement in the process of publication of the relevant words".[424] Such conduct would be seen as moving the service provider outside of the "passive, instrumental role in the process".[425]

[419] Defamation Act, supra note 417, s. 1(1)(c)
[420] Defamation Act, supra note 417, s. 2
[421] Defamation Act, supra note 417, s. 3(e)
[422] *Godfrey*, supra note 229, at 206.
[423] *Bunt v Tilley*, supra fn. 230.
[424] *Bunt v Tilley*, supra fn. 230, at [23].
[425] *Bunt v Tilley*, supra fn. 230, at [23].

Moving on to the publisher's liability of indexing services, it is worth considering the case of *Metropolitan International Schools v Designtechnica* (2009),[426] which concerned the Google Search search engine. The facts were as follows; the claimant, who provided distance learning courses in cyberspace, found out that the comments posted on an online bulletin board - hosted by the first defendant - were defaming his business. When the claimant commenced proceedings in libel, he also sued the operators of Google Search (Google UK and Google Inc) as the second and third defendants, on the basis that the defamatory material was made available through their service, in the form of 'snippets' presented below the hyperlinks. When it came to publisher's liability, Google was not regarded as a publisher of the defamatory content hosted on the websites which could be found through Google Search. The basis for this finding was that Google "has no role to play in formulating the search terms"[427] shown through its service. Consequently, "it could not prevent the snippet appearing in response to the users request unless it has taken some *positive step* in advance".[428] The judge concluded that "there being no input from the third defendant, therefore, (…), it cannot be characterised as a publisher at common law".[429] Interestingly enough, the decision also drew an analogy between Google Search and a library catalogue, stating that it would be unreasonable to hold the creators of the catalogue liable for the content of catalogued books; and that the same reasoning applies, in principle, to Google's search engine. That being said, Eady J stressed that should such a catalogue somehow include snippets along the lines of "this book includes serious allegations of corruption aimed at a well-known politician," the liability could still arise.[430]

The search engine is not the only service in relation to which Google had to appear in court, in order to deal with the claims of publisher's liability for defamatory material. In the earlier mentioned case of *Davison v Habeeb*

[426] (2009) EWHC 1765 Q.B.
[427] *Metropolitan Schools v Designtechnica*, supra fn. 426, at [51].
[428] *Metropolitan Schools v Designtechnica*, supra fn. 426 at [51], emphasis added.
[429] *Metropolitan Schools v Designtechnica*, supra fn. 426, at [51].
[430] *Metropolitan Schools v Designtechnica*, supra fn. 426, at [52].

(2011),[431] the claimant sought to make Google liable as a publisher of a defamatory blog post which appeared on Blogger.com. Upon considering this point, the court found that - at least following the notification - Google can be liable for the statement in question, as a publisher.[432] The key factors which lead to this finding were the defendant's "ability to take down offensive material"[433] and the knowledge/mental element he obtains upon being notified of the existence of the defamatory content.[434] Additionally, the judge added that as the operator of Blogger, Google "appears to assume a degree of responsibility for what is published on its Blogger.com platform. Otherwise, its contents policy is a sham".[435]

The last defamation case to be covered in this section is *Tamiz v Google* (2013).[436] This earlier mentioned[437] Court of Appeal judgment also concerned Google's liability for content posted on Blogger, but this time it was not the post itself, but the comments underneath which became a trigger for the claim of publisher's liability. At first instance, the case was struck out on the basis that Google is not the publisher of defamatory material; however, this finding was overturned on appeal. In the latter proceedings, the judge found that Google might become a secondary publisher of content, provided that it was notified about the defamatory information and did not remove it expeditiously; this was found to be the case in *Tamiz*, as five weeks passed between the notice and removal. The factors which placed Google outside of the passive facilitator role were the enablement of advertisements on the blog and the power to remove/block access to the infringing materials.[438] As for the innocent dissemination defence, Google was found to be outside of its scope

[431] *Davison v Habeeb*, supra fn. 221.
[432] *Davison v Habeeb*, supra fn. 221, at [47].
[433] *Davison v Habeeb*, supra fn. 221, at [41].
[434] *Davison v Habeeb*, supra fn. 221, at [42].
[435] *Davison v Habeeb*, supra fn. 221, at [39].
[436] *Tamiz v Google*, supra fn. 226.
[437] See chapter one, section 5.2.2.
[438] *Tamiz v Google*, supra note fn. 226, at [34].

in the same manner as Demon, the ISP from *Godfrey*; the court did not see Google's actions as representing sufficient reasonable care.[439]

Moving on to copyrighted content. While the UK legal system has not seen publisher's liability being used as a basis of claims aimed against online intermediaries whose services are used for spreading copyright-infringing content, such a use occurred in certain other EU countries – for example, in France. In the Dailymotion case from 2007,[440] the French Tribunal of First Instance (Tribunal de Grande Instance, hereafter referred to as the French TGI) refused to accept that organising advertisements on this streaming website was turning its operators into publishers; the Tribunal stated that the role of a publisher is characterised by "initiating the dissemination" of content, and Dailymotion's operators did not, according to the judges, fulfil this criterion.

The operators of the earlier mentioned[441] music streaming website Myspace were less fortunate. While the French TGI found this portal to be a hosting provider,[442] shielded from liability by virtue of art. 14 of the E-Commerce Directive,[443] it was also found to be a publisher of content, and on this basis, the French TGI stated that the operators of Myspace can be liable for the copyright-infringing conduct of their users. The operators were placed within the role of a publisher, because they went beyond mere storage and communication of content, by organising and presenting the content in a specific manner, as well attaching advertisements to the hosted content.[444]

[439] *Tamiz v Google*, supra note fn. 226, at [46].
[440] Tribunal de Grande Instance of Paris, judgment delivered on the 13th of July 2007.
[441] See chapter one, section 2.2.2.
[442] Myspace case, supra fn. 101.
[443] Myspace case, supra fn. 101 – the safe harbour provisions of the E-Commerce Directive are discussed below, in section 3.3.1 of the current chapter.
[444] Myspace case, supra fn. 101.

Moving further, we have the case of *Zadig Prods v Google Video* (2007),[445] where Google Video[446] was not classified as a publisher of content, on the basis that offering the architecture for users to classify the contents (a service "in any event necessary to render the content of the site accessible to the public"[447]) does not turn the service's operators into publishers.[448] Another case, *Flach Films v Google Video* (2008),[449] followed suit in this regard.

3.1.2. Injunctions aimed at the intermediaries.

Due to the wide variety of injunctions which can be aimed at different types of intermediaries, this section is further divided on subsections dedicated to injunctions aimed at: removing specified infringing content (section 3.1.2.1), imposing preventive content filtering schemes (3.1.2.2), and finally, blocking access to online resources used for spreading infringing content (3.1.2.3).

First of all, it is worth to note that the EU legal framework does contain legal instruments warranting the use of intermediary-focused injunctions *in general*, regardless of their type; though only in the areas of copyright law and trademark law. Art. 8(3) of the InfoSoc Directive provides that "Member States shall ensure that [copy][450]rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right".[451] The Enforcement Directive follows on, expanding (yet again) a provision of the InfoSoc Directive to IP rights in general, this time through a combination of two articles; art. 9(1)(a) and art. 11. The former provision is focused on preliminary injunctions, and states

[445] High Court of First Instance of Paris, judgment delivered on the 19th October 2007.
[446] In its old form of a video search engine and a video sharing website. This hybrid service was closed down in 2012.
[447] *Zadig Prods v Google Video*, supra fn. 445.
[448] *Zadig Prods v Google Video*, supra fn. 445. It is worth adding that Google Video ended up being liable on a different basis.
[449] Commercial Court of Paris, judgment delivered on the 20th of February 2008.
[450] (Text added by the author.)
[451] Information Society Directive, supra fn. 8, art. 8(3).

with reference to the infringer-focused injunction described above[452] that "(…) an interlocutory injunction may also be issued, under the same conditions, against an intermediary whose services are being used by a third party to infringe an intellectual property right;(…)".[453] Article 11 covers standard injunctions, providing that "(…) Member States shall also ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right, without prejudice to Article 8(3) of Directive 2001/29/EC".[454]

3.1.2.1. Removal of access to a specified piece of infringing content.

This type of an intermediary-focused injunction seems to be the first, nearly instinctive choice for the rightholders who wish to remove access to the infringing information hosted by an intermediary. The key idea here lies in forcing the service provider (who we assume to have control over the content he is hosting) to erase the illicit material or disable access to it permanently. That being said, it has to be underlined that this section covers the removal of a *specified* piece of independently infringing content, tied to a particular file/blog post/forum comment/etc., which was located by the rightholders. Injunctions aimed at removing search results leading to such content - or at forcing the intermediary to monitor his service in order to find and remove the infringing information present in other files/blog posts/etc. - have been allocated their own sections within this subchapter.

First of all, it has to be confessed that this section (belonging to the injunctions-oriented segment of the subchapter) carries a non-injunctive element, which deserves to be described first. Before moving on to the court injunctions *forcing* the intermediary to remove a specified piece of infringing content, this thesis gives attention to the notice and takedown procedures

[452] See section 2.1 of this chapter.
[453] Enforcement Directive, supra fn. 247, art. 9(1)(a).
[454] Enforcement Directive, supra fn. 247, art. 11.

(hereafter referred to as N&T), which serve the same purpose, but are capable of achieving it before any court proceedings take place.

The core idea behind the N&T schemes is rather simple; the rightholder locates on the intermediary's service a piece of information which infringes his rights, sends an infringement notice to the said intermediary, who in turn removes the illicit item from his service. Many information society service providers (general term for online intermediaries, hereafter shortened to ISSPs) have implemented fairly sophisticated N&T facilities, key examples here being Facebook,[455] Youtube,[456] or Rapidshare.[457]

In recent years, two important developments occurred in relation to notice and takedown schemes – developments noted by Urban, Schofield and Karaganis in their seminal study from 2016.[458] Firstly, the acts of both sending and processing notices are becoming increasingly automated.[459] Secondly, rightholders are more often relying on the Rights Enforcement Organisations (REOs), companies/bodies specialising in notice and takedown-based enforcement.[460]

It cannot however be denied that the reality is not as simple and conflict-free as the preceding paragraph might suggest; there are several key concerns surrounding the performance of N&T schemes, which could be directing the rightholders towards the court injunctions aimed at removal of specified infringing content. The intermediaries might (for example) want to verify the allegedly infringing character of the targeted content, what could, in the rightholder's mind, take too much time (as it happened in the earlier mentioned case of *Godfrey*[461]). Moreover, the rightholder's removal request

[455] See https://www.facebook.com/help/400287850027717/ .
[456] See http://www.youtube.com/yt/copyright/en-GB/copyright-complaint.html .
[457] See https://rapidshare.com/#help_abuse (no longer accessible).
[458] Urban JM, Karaganis J and Schofield, BL, Notice and Takedown in Everyday Practice (March 29, 2016) UC Berkeley Public Law Research Paper No. 2755628, available at SSRN: http://ssrn.com/abstract=2755628 (Publication of the Takedown Project)
[459] Urban et al, supra fn. 458, at 32.
[460] Urban et al, supra fn. 458, at 2.
[461] *Godfrey v Demon*, supra fn. 229.

might be ignored or denied (as it occurred in *Jameel*[462] and *Akanoc*[463]). Those reasons, at the very least, induce us to consider the injunctions aimed at removal of specified infringing content as well.

In a slight twist, instruments of the EU law which are directly warranting the use of such injunctions exist only within the content area of privacy; or, to be more precise – within the area of data protection. Article 12(b) of the Data Protection Directive (mentioned in the first chapter[464]), provides that individuals within the EU should be able to obtain from the data controllers the "rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive",[465] with - to remind - article 7(a) stating that personal data may be processed only if "the data subject has unambiguously given his consent".[466] It is a fairly peculiar situation for this thesis, where a specific legal provision (art. 12(b)) sets both the legal basis for identification of a given category of infringing content and establishes an enforcement scheme aimed at removing access to such content. Additionally, it is worth mentioning that this provision does not necessarily demand the use of court injunctions - upon a fitting interpretation, efficient notice and takedown scheme could potentially fulfil the requirements set by art. 12(b) as well.

It should be noted that, as far as copyright and trademarks go, injunctions discussed in this section of the chapter can also be regarded as having a harmonised EU legal basis, in the form of the earlier mentioned, broader articles of the InfoSoc and Enforcement Directives.[467] The area of defamation is the only one out of the four content types which does not have an EU-wide legal basis for such "direct removal" injunctions; though it has to remembered that the Member States' national jurisdictions are most likely to provide such a

[462] *Jameel v Dow Jones*, supra fn. 216.
[463] *Louis Vuitton v Akanoc*, supra fn. 168.
[464] See section 4.1 of chapter one.
[465] Data Protection Directive, supra fn. 181.
[466] Data Protection Directive, supra fn. 182.
[467] See the introduction to section 3.1.2 of the current chapter.

basis themselves; in fact, the reasoning presented above by Winfield and Jolowicz[468] applies to intermediary-focused injunctions as well – in principle, there is no reason why they should not be granted, including their form discussed in the current section.

Nevertheless, practice shows that across all four content areas, whenever a rightholder wishes to remove a specific piece of infringing content, he is much more likely to rely on the given intermediary's notice and takedown scheme, rather than on the corresponding injunction. Using a N&T scheme is cheaper than filing a request to the court for an injunction, it is usually quicker – and most importantly, in an overwhelming majority of cases, intermediaries are relatively keen to remove the specified bit of infringing content,[469] knowing that there is a fair amount of other, more burdensome measures which rightholders would potentially like to impose on them. Therefore, it is submitted that the role of "direct removal" injunctions is quite limited nowadays.

3.1.2.2. Preventive content filtering.

As time passed, the rightholders began to realise that the efforts aimed at removing a specific "carrier" of infringing content are likely to go beyond the point of diminishing returns;[470] primarily due to the tendency of such content to be reuploaded/shared again (quite often through the same intermediary's service), and due to the fact that keeping a watch over the content of multiple intermediaries is, without doubt, a profoundly burdensome endeavour.[471] As a result, many rightholders turned towards the idea of imposing a duty on the content-hosting intermediaries (most commonly, by means of a court injunction) to monitor their own services for infringing content and remove it

[468] Winfield and Jolowicz, supra fn. 270.
[469] Sometimes to such an extent that freedom of expression is endangered, due to the lack of sufficient verification of infringement claims, see section 3.2.1 of chapter four.
[470] Further discussed in section 4 of chapter three.
[471] In order to see how this might become a concern for the effectiveness of enforcement schemes, see sections 2.1 and 2.2 of chapter three.

upon discovery, thus eliminating the need for the rightholders to track down every single carrier of online content infringing their legitimate interests. In theory, such an approach could be employed to both prevent the infringing content complained of from reappearing on the intermediary's service, as well as to prevent the spread of infringing content which was not yet subject to the rightholder's complaint, preventing if from causing much or even any harm at all.

One of the key premises underlying such preventive filtering of content was phrased by Ginsburg, who saw the *Grokster*[472] case as a sign that the intermediaries should implement pro-active measures in order to "prevent infringement from becoming a *business asset*".[473] However, since such measures are most often much more costly and troublesome for the intermediaries than N&T schemes, the availability of court injunctions imposing preventive measures on the relevant ISSPs became one of the key conflict areas in the field of intermediary-focused injunctions.

Therefore, it is crucial for this thesis to start by determining the general attitude of the European legal framework towards preventive content filtering. On the one hand, the general idea of granting an injunction aimed at forcing the intermediary to undertake preventive measures was given the green light in the earlier mentioned trademark case of *L'Oréal v eBay*,[474] where it was stated that art. 11 of the Enforcement Directive:

- "must be interpreted as requiring the Member States to ensure that the national courts with jurisdiction in relation to the protection of intellectual property rights are able to order the operator of an online

[472] *MGM Studios v Grokster*, supra fn. 126 - Grokster's operators were found liable for the infringements of their users.
[473] Ginsburg J, 'Whose tube? Liability risks and limitations of copyright-dependent technology entrepreneurs', in Strowel A and Triaille J-P (eds), *Google et les nouveaux services en ligne* (2008), at 229, emphasis added. For further discussion of the influence of the infringement-derived profit on the online intermediaries' liability, see chapter five, section 2.3.2.2.
[474] *L'Oréal v eBay* (CJEU), supra fn. 165.

marketplace to take measures which contribute, not only to bringing to an end infringements of those rights by users of that marketplace, but also to *preventing further infringements of that kind*".[475]

According to Bonadio, the above interpretation of article 11 was a "broad and all embracing" one,[476] falling in line with recital 24 of the Enforcement Directive, which states that "depending on the particular case, and if justified by the circumstances, the measures, procedures and remedies to be provided for should include prohibitory measures aimed at preventing further infringements of intellectual property rights".[477] It is worth adding that the Court's judgment in this matter was also influenced by art. 18(1) of the E-Commerce Directive,[478] which declares that Member States' laws should provide the national courts with the option of "rapid adoption of measures, including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved".[479] Nonetheless, it should not be omitted that the CJEU in *L'Oréal* stressed that injunctions imposing preventive measures on the operators of online marketplaces (or, in the broader interpretation, on the online intermediaries in general) have to be "effective, proportionate, dissuasive and must not create barriers to legitimate trade".[480]

However, on the other side of the cited provisions and paragraphs lies article 15(1) of the E-Commerce Directive, which states that:

- "Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14,[481] to

[475] *L'Oréal v eBay* (CJEU), supra fn. 165, at [H13(7)] and [131], emphasis added.
[476] Bonadio E, 'Trade marks in online marketplaces: the CJEU's stance in L'Oréal v eBay.' (2012) C.T.L.R. 18(2), 37, at 41.
[477] Enforcement Directive, supra fn. 247, rec. 24. This provision was, in fact, referred to by the CJEU, at [134].
[478] *L'Oréal v eBay* (CJEU), supra fn. 165, at [132].
[479] E-Commerce Directive, supra fn. 91, art. 18(1).
[480] *L'Oréal v eBay* (CJEU), supra fn. 165, at [144].
[481] Definition of such services is covered by art. 2(a) of the E-Commerce Directive.

> monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity".[482]

It is quite remarkable how this provision (further covered in section 3.3.2 of the current chapter) states that the relevant ISSP shall not be obliged to conduct activities which are arguably the prime methods of achieving the aim of preventing infringement through the online intermediaries, the aim which was broadly supported by the judgment in *L'Oréal* and by the EU legislation cited above. And in fact, art. 15 has proven to be one of the key obstacles lying in the way of rightholders wishing to impose preventive filtering duties on the ISSPs - as it will be shown in the following paragraphs, which describe four cases of claimants wishing to impose preventive measures (centred around the concept of content filtering) on the relevant intermediaries.

The first and foremost of those decisions is the CJEU case of *Netlog*. As mentioned earlier,[483] the proceedings in question concerned a social media website, the users of which shared copyright-infringing material through the website's video-streaming facilities. SABAM, the claimant agency representing the copyrightholders, requested "that Netlog be ordered immediately to cease unlawfully making available musical or audio-visual works from SABAM's repertoire".[484] According to the Court, this was tantamount to a request for a filtering system: one covering all the service's users indiscriminately, as a preventative measure, exclusively at the hosting providers' expense and for an unlimited period of time. Such a form of a content filtering order was seen by the Court as a general monitoring obligation, going against art. 15 of the E-Commerce Directive.[485]

[482] E-Commerce Directive, supra fn. 91, art 15(1).
[483] See section 2.2.2 of chapter one.
[484] *SABAM v Netlog*, supra fn. 103, at [26].
[485] *SABAM v Netlog*, supra fn. 103, at [38].

In the case of *Telecinco v Youtube*,[486] the claimant (relying on articles 138 and 139 of the Spanish Copyright Act[487]) sought to obtain an injunction which would be forcing Youtube to actively monitor the files uploaded by its users in search of the claimant's copyrighted content. However, the judge dismissed this request (as did the Court of Appeal later on), finding the defendant to be an intermediary within the meaning of the E-Commerce Directive[488] (and, accordingly, its art. 15), and thus stated that:

- "Youtube is not a content provider and, therefore, is not obliged to supervise in advance the lawfulness of such contents which are hosted on its website; its only obligation is precisely to cooperate with the rights holders as to proceed, when the infringement has been identified, to immediately remove the contents".[489]

As we can see, after denying the option of preventive content filtering, the judge pointed to the notice and takedown procedure as the primary (if not the only) alternative to the former measure. Interestingly enough, he justified such reasoning with the following words;

- "It is true that we must agree that it [the N&T scheme][490] is not a handy and easy procedure for the plaintiff, particularly because it bears the hard task of tracing and checking the contents which are hosted on the defendant's website. However, this is due precisely to the order of priorities which both the Community and the national legislator have established".[491]

[486] *Telecinco v Youtube*, supra fn. 83,and section 2.2.2 of chapter one,
[487] Ley 22/1987 de 11 de noviembre, de Propiedad Intelectual.
[488] E-Commerce Directive, supra fn. 91.
[489] *Telecinco v Youtube*, supra fn. 83.
[490] Words added by the author.
[491] *Telecinco v Youtube*, supra fn. 83.

The third example of a case where a claimant sought to impose preventive filtering duties on an ISSP is the decision in *Atari v Rapidshare*,[492] introduced above, in section 2.2.1 of chapter one. The claimant video game company (relying on the premise that online pirates are going to share their product through files containing the game's name in title) applied for an injunction forcing Rapidshare to filter their hosted content in order to locate and delete files which include specific keywords – such as, for example, "Alone in the Dark". However, this application was dismissed by the judge due to two primary factors.

First of all, the court refused to accept the idea that the presence of such keywords constitutes sufficient evidence of the infringing character of the content in question, and added that the users themselves are not dependent on such keywords.[493] The court rightly pointed out that the said users obtain the links to the infringing files from external websites, what in essence means that an infringing file can be uploaded to Rapidshare under the name of "123123123.zip" and it will not make much of a difference. The second factor underlying the court's reasoning stems, in a way, from the first one – assuming the presence of a keyword (such as the game's title) does not warrant the deletion of a file bearing it, the judge inferred that manual verification of files would be required. However, he refused to place such a requirement on Rapidshare's operators, stating that it would be an unduly onerous activity,[494] its costs likely to be increased by the variety of keywords which were potentially likely to be used by the uploaders in order to characterize the claimant's content.[495]

However, this decision has to be seen now in the light of the German Supreme Court (hereafter referred to as the BGH) judgment in the case of *GEMA v*

[492] *Atari v Rapidshare*, supra fn. 49, the case was also mentioned in section 2.2.2 of chapter one.
[493] *Atari v Rapidshare*, supra fn. 49, at [32].
[494] For further discussion of the allocation of burden within the enforcement schemes, see chapter four, section 3.3.
[495] *Atari v Rapidshare*, supra fn. 49, at [33].

Rapidshare (2013).[496] While the latter concerned music files, as opposed to video games, the key issue remained the same; should the operator of a cyberlocker be required to actively search for infringing content in order to prevent his service from being used for infringing purposes? The BGH answered this question affirmatively, stating that Rapidshare's business model "contains an inherent structural danger of large-scale copyright infringements to such an extent that significantly increased obligations of due diligence and duty to act measures to prevent copyright infringements".[497] Instead of a narrow keyword filter which was sought in *Atari v Rapidshare*, the injunction granted in *GEMA v Rapidshare* obliged the operators of this cyberlocker to "find out through general search engines like Google, Facebook, or Twitter using applicably formulated search enquiries and, where appropriate, also so-called web crawlers, whether references to further infringing links to Defendant's service can be found (…)".[498] It has to be added that the term "infringing links" indicates here the specific copyrighted works about which GEMA complained, it was not a blanket injunction related to all forms of infringing content.

These are just four out of many cases where the rightholders sought to obtain an injunction aimed at imposing preventive filtering measures on content hosting intermediaries. It seems plausible to state that at the moment, such preventive filtering injunctions are fairly difficult to obtain - across all four content types (art. 15 of the E-Commerce Directive[499] does not differentiate between categories of content, relying instead on the broad term "illegal activity"[500]). Additionally, there is a visible lack of guidance from the CJEU with regards to the acceptable shape of a content filtering injunction; though decision of the BGH might be indicating that at least in the area of copyright, some Member States might be moving towards this method of online enforcement.

[496] BGH, 15 August 2013, I ZR 80/12.
[497] *GEMA v Rapidshare*, supra fn. 496, at [13].
[498] *GEMA v Rapidshare*, supra fn. 496, at [60].
[499] Described in section 3.3.2 of the current chapter.
[500] E-Commerce Directive, supra fn. 91, art. 15(1).

However, just as the intermediary-ran N&T schemes described above[501] are the voluntary, more cooperative form of the injunction aimed at the removal of specified content, it has to be mentioned that on rare occasions, certain ISSPs voluntarily undertake preventive filtering measures themselves: most notably Youtube, the earlier mentioned streaming website, which implemented the so-called Content ID system. Here, the process starts with copyrightholders providing Youtube with the reference files (audio or audiovisual) of their works. New videos uploaded to the website are then automatically compared with such files. The next step is where Content ID differs from the traditional idea of preventive filtering, focused on straightforward removal of access to infringing content. The copyrightholders can request the system to perform one of the three actions once it discovers a video matching their reference file(s) (ie. a video most likely to be infringing their rights). Such a video might be blocked (which is the closest option to traditional removal), monetised (through adding adverts to the video, the profit from which is directed to the copyrightholder) or tracked (by granting the rightholder access to the video's viewership statistics).[502]

Content ID could be classified by some as a form of quasi-preventive filtering; after all, the copyrightholders still have to contact Youtube and provide them with necessary reference files. Then again, it is most likely not possible to conduct preventive filtering without some form of direct or indirect notification from the rightholders.[503] Nevertheless, however we classify it, Content ID has to be given credit for going beyond mere removal of infringing content, and adopting a more cooperative approach to this problem. The downside here is that so far, Content ID is only applied in the area of copyright-infringing content; the three other content types are outside of its scope - and while trademarks could, in theory, be covered by a similar filtering

[501] See section 3.1.2.1 of the current chapter.
[502] See http://www.youtube.com/t/contentid .
[503] See section 2.3.1.2 of chapter five for further discussion of this issue.

scheme, it is fairly difficult to imagine Content ID being used to deal with text-based defamatory or privacy-infringing content.

3.1.2.3. Blocking access to online resources used for spreading infringing content.

This section of the subchapter could be seen as a step up on the ladder of stigma carried by intermediary-focused injunctions. Here, the rightholders no longer contact the intermediary whose service is being used to host/share the infringing content – instead, they turn their attention towards the other intermediaries connected to their targeted online service provider, ones who are capable of impairing access to it.[504] In recent years, injunctions purporting to achieve this aim have become increasingly popular – though yet again, primarily in the area of intellectual property, with copyright law being the unquestionable leader. It should be fairly clear at this point of the thesis that amongst the four covered categories of rightholders, the copyright owners exhibit a considerable degree of "eagerness" (probably connected to the amount of available resources) when it comes to endorsing a wide variety of enforcement schemes presented in this chapter.

As far as the EU legal framework is concerned, there is no harmonised legal basis specifically warranting the use of such injunctions in general - and there are not many Member States whose legal systems contain it. One of those few who do is, providentially for this thesis, the United Kingdom, whose Digital Economy Act 2010 (hereafter referred to as the DEA 2010, and mentioned above for its provisions related to the graduated response[505]) provided for the use of blocking injunctions in its section 17. While, as it will be shown in section 3.1.2.3.1 of the current chapter, the UK courts granting the ISP-

[504] It has to be underlined that in the real world, it is most likely the case that the intermediaries care less about this kind of a stigma than they do about more pragmatic considerations, such as the costs of maintaining N&T and/or a preventive filtering scheme – see section 3.3 of chapter four.
[505] DEA 2010, supra fn. 332 and section 2.4 of chapter 2.

oriented blocking orders rely on s. 97A of the CDPA 1988, and s. 17 of the DEA 2010 was repealed by the Deregulation Act 2015,[506] it can still be seen as a good, robust example introducing the landscape of blocking injunctions.

By virtue of this section, the Secretary of State could have introduced regulations explicitly providing the courts with an option of granting a blocking injunction against a "location on the internet" (most commonly, a website) which the court sees as "(…) being, or (…) likely to be used for or in connection with an activity that infringes copyright".[507] The online service provider who received the blocking injunction would have to "prevent its service being used to gain access"[508] such a location. However, before the court granted such an injunction, it would have to be satisfied that its subject is:

- "(a) a location from which a substantial amount of material has been, is being or is likely to be obtained in infringement of copyright,
- (b) a location at which a substantial amount of material has been, is being or is likely to be made available in infringement of copyright, or
- (c) a location which has been, is being or is likely to be used to facilitate access to a location within paragraph (a) or (b)".[509]

Moreover, when deciding whether a blocking injunction should be granted, the court should take into account the following five factors:

- "(a) any evidence presented of steps taken by the service provider, or by an operator of the location, to prevent infringement of copyright in the qualifying material,
- (b) any evidence presented of steps taken by the copyright owner, or by a licensee of copyright in the qualifying material, to facilitate lawful

[506] Deregulation Act 2015, c.20, s. 56.
[507] DEA 2010, supra fn. 332, s. 17(1).
[508] DEA 2010, supra fn. 332, s. 17(2).
[509] DEA 2010, supra fn. 332, s. 17(4). Point (c) is quite clearly pointing towards the indexing services, which are covered in greater detail in section 3.1.2.3.3 of the current chapter.

access to the qualifying material,

- (c) any representations made by a Minister of the Crown,
- (d) whether the injunction would be likely to have a disproportionate effect on any person's legitimate interests, and
- (e) the importance of freedom of expression".[510]

It seems plausible to state that in the current setting, it is fairly difficult to introduce legislative instruments aimed at regulating the use of intermediary-blocking injunctions. However, this does not mean that the road to obtaining such court orders is closed for the rightholders; quite the contrary, the recent years saw an increase in the number of claimants (again, pretty much exclusively from the copyright area) seeking such injunctions on the basis of the already existing laws – and quite often, successfully obtaining them, as the following subsections are going to demonstrate. The intermediary-blocking injunctions presented here have been divided into three categories, each of them tied to a specific type of a service provider capable of blocking access to the online resources used for sharing content which infringes the legitimate interests of the rightholders.

3.1.2.3.1. Blocking access to online resources through the Internet Service Providers.

Among the intermediaries present in section 3.1.2.3 of the current chapter, the Internet Service Providers (ISPs) could be seen as holding a fundamental position, due to their principal service of providing their subscribers with the basic connection to the Internet. It is through the ability to influence the said connection that the ISPs can, for example, attempt to block access to websites or P2P networks used for spreading infringing content. The following paragraphs present a selection of instances where rightholders sought to obtain a court order in UK, obliging the ISPs to use their power for this exact purpose.

[510] DEA 2010, supra fn. 332, s. 17(5).

The first of those instances is the landmark case of *Twentieth Century Fox Film Corp v British Telecommunications Plc* (2011)[511] (hereafter referred to as *Fox v BT* or the Newzbin2 case), which followed the earlier mentioned judgment in *Twentieth Century Fox Film Corp v Newzbin*[512] (hereafter referred to as *Fox v Newzbin*). In the latter decision, Newzbin was not only found to be liable in damages for the infringements of its users,[513] but was also subjected to an injunction forcing the website's operators to filter the search results shared through their platform, in search of the links leading to the claimant's copyrighted works. Now, while this injunction is further described in section 3.1.3.3 below, in order to understand the case of *Fox v BT*, let us turn our attention towards the immediate consequences of the injunction granted in *Fox v Newzbin*. Together with the financial burden of the legal proceedings, it prompted the reincarnation of the Newzbin website as Newzbin2, which inherited much of Newzbin's infrastructure and user base. Newzbin2 appeared shortly after the judgment in *Fox v Newzbin*, and was established by a group known as Team R Dogs.

Upon noticing the reinstatement of the convicted website, Fox decided to change the approach and, through the case of *Fox v BT*, applied for a blocking injunction against Newzbin2, based on section 97A of the CDPA 1988.[514] This provision of the UK law, giving effect to art. 8(3) of the InfoSoc Directive,[515] states that "the High Court (in Scotland, the Court of Session) shall have power to grant an injunction against a service provider, where that service provider has actual knowledge of another person using their service to infringe copyright". Here, the requested injunction was aimed at forcing BT (the largest ISP in UK) to prevent its subscribers from accessing the Newzbin2 website. It is worth outlining three aspects of the judgment which led to the award of the sought injunction. First of all, BT accepted that it was a service

[511] [2011] EWHC 1981 (Ch).
[512] *Fox v Newzbin*, supra fn. 122.
[513] See section 3.1.1 of the current chapter.
[514] CDPA 1988, supra fn. 253, s. 97A.
[515] Information Society Directive, supra fn. 8, art. 8(3).

provider within the meaning of s. 97A.[516] Secondly, the ISP was found to have been used for the purpose of infringing copyright by both the operators of Newzbin2, as well as by the website's users (as far as those users were BT's subscribers).[517] And thirdly, while the defendant was not shown to have actual knowledge of each particular infringement committed through the indexing website in question, BT was found to possess the actual knowledge of its services being used for infringing purposes; Arnold J stated that the defendant ISP:

- "knows that the users and operators of Newzbin2 infringe copyright on a large scale, and in particular infringe the copyrights of the Studios in large numbers of their films and television programmes, it knows that the users of Newzbin2 include BT subscribers, and it knows that those users use its service to receive infringing copies of copyright works made available to them by Newzbin2"[518]

Such knowledge was found to be sufficient for the purpose of s. 97A – and hence, primarily on the basis of this and the other two described findings, the requested injunction was granted.[519] Additionally, it is worth adding that it was extended to cover "any other IP address or URL whose sole or predominant purpose is to enable or facilitate access to the Newzbin2 website".[520]

The judgment in *Fox v BT* became the point of reference for the copyrightholders wishing to block access to other "pirate" websites in the UK. One of the first cases which relied on this point of reference in order to secure the award of a blocking injunction was *Dramatico Entertainment v British Sky Broadcasting (No. 2)*(2012).[521] The factual background of this case was similar to the Newzbin cases; but with the same roles played by different

[516] *Fox v BT*, supra fn. 511, at [H12].
[517] *Fox v BT*, supra fn. 511, paras [100] – [113].
[518] *Fox v BT*, supra fn. 511, at [157].
[519] *Fox v BT*, supra fn. 511, at [204].
[520] *Fox v BT*, supra fn. 511, at [260].
[521] *Dramatico v Sky (No. 2)*, supra fn. 117.

actors. Instead of a film company, the claimants were representing the music industry; the defendants were not one, but six major UK ISPs (including BT); and instead of a Usenet-indexing website, the target of the injunction was a BitTorrent focused one – the well-known by this point of the thesis, The Pirate Bay.

In the preliminary case of *Dramatico Entertainment Ltd v British Sky Broadcasting Ltd (No. 1)* (2012)[522] both users and operators of The Pirate Bay were found to be engaging in activities infringing the claimants' copyrights.[523] The subsequent case of *Dramatico Entertainment v British Sky Broadcasting (No. 2)* focused purely on the grant of a blocking injunction. This time, there was no challenge made to the notion that the ISPs' services are used for the infringing purposes, nor did they try to deny the possession of the actual knowledge of the infringements – hence, the injunction was granted without any noticeable legal obstacles.[524]

It is worth mentioning here two other UK cases which followed *Dramatico Entertainment v British Sky Broadcasting (No. 2)* in awarding similar injunctions under s. 97A of the CDPA 1988. Firstly, the decision in *EMI Records Ltd v British Sky Broadcasting Ltd* (2013) saw the successful application for a blocking injunction against three further BitTorrent websites (known as Kickass Torrents, H33T and Fenopy).[525] Secondly, the (illicit) football streaming website known as FirstRow Sports was subjected to a blocking injunction as a result of the application made by the Football Association Premier League in the case of *Football Association Premier League Ltd v British Sky Broadcasting Ltd & Others* (2013).[526] Additionally, in a (so far) rare trademark case of *Cartier International AG v British Sky Broadcasting Ltd* (2014),[527] a number of websites advertising and selling

[522] [2012] EWHC 268 (Ch).
[523] *Dramatico v Sky (No. 1)*, supra fn. 522, at [82].
[524] *Dramatico v Sky (No. 2)*, supra fn. 117, at [5] - [6].
[525] *EMI v Sky*, supra fn. 119.
[526] [2013] EWHC 2058 (Ch).
[527] [2014] EWHC 3354.

counterfeit goods was blocked in a similar way on the basis of the generic s. 37 of the Senior Courts Act 1981[528], which states that "(t)he High Court may by order (whether interlocutory or final) grant an injunction or appoint a receiver in all cases in which it appears to the court to be just and convenient to do so".

While this thesis relies on the UK as a primary example of a Member State jurisdiction, it should be underlined that applications for blocking injunctions (of the same kind as described in the preceding paragraphs) have been made in quite a few other jurisdictions of the European Union. Cases such as *IFPI Danmark v Tele 2 A/S* (2006)[529] (Denmark), *Columbia Pictures Industries Inc v Portlane AB* (2010)[530] (Sweden) or *Constantin Film v UPC* (2011)[531] (Austria) saw the award of such injunctions aimed at websites used for copyright-infringing purposes. On the other hand, the claimants were not as successful in *Nordic Records Norway AS v Telenor ASA* (2010)[532] (Norway) or *Stichting Bescherming Rechten Entertainment Industrie Nederland (BREIN) v Ziggo BV* (2010)[533] (Netherlands), where corresponding applications were dismissed – though it has to be underlined that the latter two decisions dealt with the requests for preliminary/interim injunctions.

Analysing and comparing the decisions cited in the preceding paragraph would be, without doubt, a worthy academic exercise, which could potentially reveal certain patterns in the European judges' reasoning in such cases. However, for this thesis, it is largely sufficient to keep in mind that such blocking injunctions are in use, and are likely to grow in popularity due to the considerable success rate of claims aimed at obtaining them.

[528] Senior Courts Act 1981 c. 54.
[529] 25 October 2006, Copenhagen City Court.
[530] 4 May 2010, Swedish Court of Appeal.
[531] 13 May 2011, Commercial Court of Austria.
[532] 9 February 2010, Borgarting Court of Appeal.
[533] 19 July 2010, District Court of the Hague.

So far, this section focused on website-blocking injunctions, which are the primary type of a court order requiring the ISPs to block access to an online resource. Nevertheless, it should be also mentioned here that there were some attempts in the EU to impose on the ISPs the duty to block access to P2P networks[534] in a direct manner, that is, for example, by preventing their subscribers from being able to use such networks. The chief example of such an attempt is the CJEU case of *Scarlet Extended v SABAM* (2011),[535] mentioned in the first chapter of thesis.[536] The following paragraph focuses on the court order which SABAM tried to obtain[537] in order to prevent the infringement of its members' copyright by P2P filesharing.

The order which was awarded by the President of the Tribunal of the First Instance in Brussels obliged Scarlet to "bring to an end the copyright infringements established in the judgment of 26 November 2004 by making it impossible for its customers to send or receive in any way files containing a musical work in SABAM's repertoire by means of peer-to-peer software, on pain of a periodic penalty".[538] If we were to dissect this injunction, it could be seen as consisting of four steps. First of all, Scarlet (the ISP) would have to identify within the traffic of its subscribers all files transferred through the P2P networks. Those files would then have to be examined in order to discover whether any of them contains the claimant's copyrighted works. Consequently, the ISP would have to decide whether the identified copyrighted works are shared illegally, and finally, the ISP would have to block the sharing of the illicit material located in the earlier mentioned manner.[539]

[534] (Used for copyright-infringing filesharing.)
[535] *Scarlet Extended v SABAM*, supra fn. 105.
[536] See section 2.2.3. of chapter one.
[537] (And in the Belgian court of the first instance, did in fact obtain.)
[538] *Scarlet Extended v SABAM*, supra fn. 105, at [23].
[539] For the analytical background of this paragraph, see Opinion of Mr Advocate General Cruz Villalón in the Case C-70/10, delivered on 14 April 2011, [53] to [65].

Upon being asked for opinion on whether such an injunction is compatible with the EU law, CJEU answered negatively, stating that:

"in adopting the injunction requiring the ISP to install the contested filtering system, the national court concerned would not be respecting the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business,[540] the right to protection of personal data[541] and the freedom to receive or impart information,[542] on the other".[543]

It is worth adding here that, as Sanders noted, the Belgian court did not give a specific guidance on what kind of a filtering system should be used by Scarlet, or how the (infringing) content should be identified.[544] It seems plausible to state that following the discussed case, the requests for a similar injunction, phrased in similarly broad terms, are unlikely to succeed within the borders of the EU.

3.1.2.3.2. Blocking access to online resources through the operators of the Domain Name System servers and the domain name registrars.

In order to understand the injunctions covered in this section, which focus on the operators of the DNS servers and the domain name registrars, it is necessary to begin by understanding what the Domain Name System (DNS) actually is. Whenever an Internet user's computer wishes to connect to a website, it (in principle) requires this website's IP address. However, due to the fact that the IP addresses are fairly inconvenient in use (being rather long

[540] The case contains the further discussion of this legitimate interest at [48].
[541] The case contains the further discussion of this legitimate interest at [50].
[542] The case contains the further discussion of this legitimate interest at [50].
[543] *Scarlet Extended v SABAM*, supra fn. 105, at [53]. Further discussion of the cited human rights can be found in chapter four.
[544] Sanders A, 'Intellectual property liability of consumers, facilitators and intermediaries: Comparative Concepts', in Heath C and Sanders A (eds), Intellectual property liability of consumers, facilitators and intermediaries (2012), at 13.

and indistinct), the DNS was developed. This system provides the means for allocation of the word-based domain names to websites' numeric IP addresses, directing users who type in the former, to the latter. By way of example; the University of Nottingham website's IP address is 128.243.80.167, and its domain name is http://www.nottingham.ac.uk/. In a way, the DNS could be seen as a form of an interactive phone book of the World Wide Web, where we can just use the name of a person/establishment instead of typing their whole phone number.

The blocking injunctions focused on the operators of the DNS servers and the domain registrars are aimed at severing the connection between the targeted website's domain name and its IP address, thus preventing the online users from accessing the website through its domain name. While the former category of intermediaries can only be asked to refrain from processing the Internet users' requests of access to the targeted location, the latter can be asked to remove the connection between the IP address and the domain name completely, by ceasing to provide such a service to its client (ie. the targeted website).

There is a certain similarity here with the ISP-orientated measures described in section 3.1.2.3.1 above – the Internet Service Providers can also block a given website's domain name; though on a slightly different level. They can prevent the domain name from being operative for their subscribers, what is contrasted with the DNS server operators' ability to sever the domain name-IP address connection for the whole of the traffic passing through their service and the domain name registrars' power to seize the domain name in question.

As far as the four content types covered by this thesis are concerned, the injunctions directed at the DNS server operators or domain name registrars are only becoming noticed within the European Union. However, they have been fairly popular in the US, which can provide examples showing the use of this blocking measure.

In the American jurisdiction, the domain names of copyright and trademark-infringing websites are actually, at times, seized by way of an injunction forcing the domain name registrars[545] to assign the relevant domain names to the authorities. The legal basis for such a seizure lies in section 2323 of the United States Code, which provides that the US government may seize "any property used, or intended to be used, in any manner or part to commit or facilitate the commission (…)"[546] of a range of copyright and trademark offences,[547] as well as force someone convicted of those offences to forfeit such property to the same authorities. In this regard, the discussed seizures could be also used as an example within section 3.2 of the current chapter.

The cited provision was relied on a number of occasions of interest to this thesis; the most prominent one being the so-called "Operation in our Sites". It is an ongoing undertaking conducted by the U.S. Immigration and Customs Enforcement agency (hereafter referred to as the ICE). The key part of this operation is formed by systematic seizures of the domain names used by websites connected to copyright and/or trademark infringing activities. For example, during the so-called "Cyber-Monday crackdown," the ICE seized 82 domains of websites belonging to the earlier mentioned category.[548] On a different occasion, ICE seized the domain names of eleven Korean websites facilitating the pirate downloads of copyrighted movies.[549]

It is worth adding here that this method of enforcement might be gaining some recognition in the UK; in October 2013, the Intellectual Property Crime Unit of the City of London Police (hereafter referred to as the PIPCU) began asking

[545] Such as GoDaddy.com, Inc or eNom, Inc.
[546] United States Code, Title 18, Part I, Chapter 113, §2323 (a)(1)(B).
[547] Being more specific, the offences set out in section 506 of title 17, sections 2318, 2319, 2319A, 2319B and 2320 of chapter 90, of the same title.
[548] See http://www.ice.gov/news/releases/1011/101129washington.htm. Seized domain names included, for example, "louisvuittonoutletstore4u.com" and "torrent-finder.com".
[549] See http://torrentfreak.com/feds-seize-domains-of-korean-movie-portals-111204/. Seized domain names included sites such as "82movie.com" or "007disk.com".

the domain name registrars to suspend the domain names of websites used for facilitating copyright infringement (most notably, torrent websites).[550]

As far as the operators of the DNS servers are concerned, they have not really come under the crosshair of court injunctions, whether in US or anywhere else. That being said, they should not be omitted here due to the obligations which could be placed on them by the potential spiritual successors of the USA's (dismissed) bill known as the Protect IP Act 2011.[551]

3.1.2.3.3. Blocking access to online resources through the providers of indexing services.

The third category of entities which became subjected to enforcement efforts aimed at removing access to online locations (most commonly, websites) facilitating the exchange of infringing content are the providers of various indexing services, such as search engines or online forums. In principle, the term "indexing service" (as used in this thesis) could actually cover multiple online services which facilitate the Internet users' access to another service used for sharing infringing content – and it has to be remembered that the latter could be an indexing service itself. A situation demonstrating such a scenario could be that of a search engine being asked to remove a search result leading to an online forum indexing cyberlocker content.

The enforcement approach discussed in this section incorporates treating the indexing information with the same measures as the infringing content it leads to; measures presented above in sections 3.1.2.1 (removal of specified infringing content) and 3.1.2.2 (preventive content filtering). It should be noted here that the line between indexing information and infringing content might become slightly blurry at times – especially when we consider

[550] See https://torrentfreak.com/uk-police-orders-registrars-to-suspend-domains-of-major-torrent-sites-131009/

[551] (Proposed) S. 968 (112th): Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011.

defamatory and privacy-infringing content, as well as (to an extent) trademark-infringing content. It is less of a case for copyright-infringing material, where, for example, a link to an infringing movie hosted on Rapidshare cannot really be held to reproduce or communicate the infringing content independently of the indexed file.

Regardless of how blurred this line becomes, it seems plausible to state that the enforcement approach at hand has become quite popular amongst the rightholders. Therefore, this section provides brief descriptions of three representative instances in which the claimants sought to strike at the indexing information leading to online resources used for sharing content which infringed upon their interests.

The first of them revolves around the notion of the N&T schemes operated by indexing services. The core idea behind this enforcement mechanism was described in section 3.1.2.1 of the current chapter– the difference being that the focus changes from notices about the infringing content *per se*, to notices about the indexing information leading to it. It is hard to come up with a more notable example here than the N&T scheme conducted by the largest search engine in cyberspace, which is Google Search. If we look at the notices of copyright infringement alone, between January and July 2013, Google Search received over 100 million of them.[552] Two of numerous thesis-relevant examples which contributed to this number could be the removal of H33T (a torrent search engine)[553] from Google's search results following the request filed in by HBO,[554] or the delistment of KickassTorrents (as one could guess, another torrent website)[555] following the notice filed in by the Motion Picture Association of America (hereafter referred to as the MPAA).[556] Furthermore, to provide an example from a different content area; the data protection/privacy-oriented procedure warranted by the *Costeja*[557] case

[552] See http://www.bbc.co.uk/news/technology-23489363
[553] *EMI v Sky*, supra fn. 119.
[554] See https://torrentfreak.com/hbo-gets-google-to-remove-h33t-homepage-130601/.
[555] *EMI v Sky*, supra fn. 119.
[556] See http://torrentfreak.com/mpaa-kicks-kickasstorrents-off-google-with-precision-takedown-130623/.
[557] *Costeja*, supra fn. 196.

(described in chapter one, section 4.2.2) also involves the application of the discussed scheme; though only in relation to indexing information based on the complainant's name.

As it was mentioned above, the notion of preventive filtering has, in recent years, extended its reach to the indexing information. Presented below are two UK cases through which the rightholders sought to impose preventive filtering obligations on the providers of indexing services.

The first one of them is *Metropolitan v Designtechnica* (2009),[558] the facts of which were presented above,[559] where the case was analysed from the angle of publisher's liability. Importantly for this section of the thesis, the claimant sought, inter alia, to obtain "an injunction to restrain the second and third defendants whether by themselves, their servants or agents, subsidiaries or otherwise, from publishing or causing to be published or authorising to be published the same or similar words defamatory of the claimant within the jurisdiction of the court".[560] In practice, this could be translated into a request for preventive filtering of the search engine's search results – a request which ended up being dismissed, since it was dependent on finding Google Inc. liable as the publisher, and Eady J found that (in the factual circumstances at hand) the search engine operator cannot be subjected to such liability and suggested that the application for injunctive relief should be directed towards the first defendant instead.[561]

Metropolitan could be seen as a sign of reluctance on the part of the UK courts to impose preventive filtering obligations on the operators of indexing services - however, such an assumption should be seen in the light of the case of *Fox v Newzbin*, where (as it was mentioned in section 3.1.2.3.1 of the current chapter) the said obligations were in fact imposed on the operators of the Usenet-indexing service.

[558] *Metropolitan v Designtechnica*, supra fn. 426.
[559] See section 3.1.1.4 of the current chapter.
[560] *Metropolitan v Designtechnica*, supra fn. 426, supra fn. 558, at [59].
[561] *Metropolitan v Designtechnica*, supra fn. 426, at [62] – [64].

Interestingly enough, the claimants in this case applied for two filtering injunctions. The first one was concerned with filtering the indexing information in order to prevent the claimant's works from being illegally shared through Newzbin. This was the injunction that was granted by Kitchin J, on the basis of finding that:

"It is the defendant's intention to make available through Newzbin all films posted on Usenet, so inevitably including the copyright films in the claimants' repertoire both now and in the future. This plainly constitutes a general threat to infringe the claimants' present and future copyrights. I also have in mind Mr Clark's unchallenged evidence that it would be a straightforward exercise for the defendant to filter the content of Newzbin by reference to a database provided by the claimants. (…)".[562]

The second claim for injunctive relief was not as successful as the first one. By reference to section 97A of the CDPA 1988,[563] Fox sought to obtain a much broader "(…) injunction to restrain the defendant from including in its indices or databases entries identifying any material posted to or distributed through any Usenet group in infringement of copyright".[564] The judge dismissed this claim. First of all, the injunction applied for was found to be too broad, encompassing works to which the claimants did not hold the rights, which goes against the reasoning of art. 8(3) of the Infosoc Directive.[565] Secondly, according to Kitchin J, it was not proven that the defendant possesses knowledge of all infringements occurring through their website; as a result, the court found that it does not have the jurisdiction required to grant this injunction. Thirdly, the rights of other potential rightholders which would be covered by the requested injunction were found to be undefined (in contrast to those of the claimant), and hence, the grant of the injunction would be likely to cause significant legal uncertainty.[566]

[562] *Fox v Newzbin*, supra fn. 122, at [129].
[563] CDPA 1988, supra fn. 514.
[564] *Fox v Newzbin*, supra fn. 122, at [133].
[565] Supra fn. 8 – art. 8(3) is implemented into the UK law through s. 97A of the CDPA 1988.
[566] *Fox v Newzbin*, supra fn. 122, at [135].

As much as effectiveness is primarily a concern of chapter three, it might be mentioned here that it is fairly clear that the creation of Newzbin 2 (which was subjected to a blocking injunction described above[567]) undermined, to an extent, the approach based on imposing preventive filtering obligations on indexing websites' operators: particularly where the targeted service is primarily used for infringing purposes. In any case, the conclusion that can be made in the current section of the chapter is that if appropriately specified,[568] the discussed type of a preventive injunction can be obtained by the (copy)rightholders - though such a feat becomes more difficult to perform when the defendant operates an indexing service of a more generic character, one which is used for significant legitimate purposes and is operating with a minimum amount of human interference.

3.2. Subjecting the intermediaries to criminal liability.

As it was shown in section 2 of the current chapter, certain types of infringers can be subjected to both civil and/or criminal liability; and the same holds true when looking towards the relevant online intermediaries. The increasing reliance on criminal law in the discussed area fits in with the remark made by Urbas in 2012, when he noted (in the context of copyright) that the global trend for enforcement efforts is to go more and more punitive, with the increasing use of measures tied to the concept of criminal liability.[569]

Similarly to the infringer-focused counterpart of this section, the efforts within the legal systems of the EU and the UK to impose criminal liability on online intermediaries whose services were used for spreading infringing content focused around copyright- and trademark-infringing content. That being said, it is worth underlining that when we consider online intermediaries, the array

[567] In section 3.1.2.3.1 of the current chapter.
[568] For example, not aimed at a whole category of infringing content.
[569] Urbas G, 'Copyright, crime and computers: new legislative frameworks for intellectual property rights enforcement.' (2012) J.I.C.L.T. 7(1), 11, at 23.

of measures warranted by the stamp of criminal liability expands; apart from the prison sentences and fines, confiscation of property such as the website's domain name[570] (or servers on which the said website is hosted) opens new avenues of enforcement, which do not arise within the infringer-oriented enforcement efforts.

Just as it was with the criminal liability of relevant infringers, EU law does not contain a harmonised legal basis for the imposition of such liability on online intermediaries. As for international law, art. 61 of TRIPS 1994 (presented and discussed above[571]) applies here as well: in a potentially more confident manner, due to the fact that the term "commercial scale" seems to be more suited to online intermediaries rather than to individual infringers using those intermediaries' services.

Once again, due to the lack of relevant provisions of the EU law, it is particularly worthwhile to look towards the UK and the criminal enforcement efforts undertaken there against the relevant online intermediaries. To this end, this section discusses two modes of criminal liability which were put to the forefront of the enforcement strategy in question; the modes of liability imposed through the common law offence of conspiracy to defraud and the offence set out in section 107(2A) of the CDPA 1988.[572]

3.2.1. Conspiracy to defraud.

Starting with the former, which bears a degree of resemblance to joint tort liability: the key definition of conspiracy to defraud was given in the case of *Scott v Commissioner of Police of the Metropolis* (1974),[573] where Viscount

[570] See section 3.1.2.3.2 for the initial discussion on how domain names can be used within the enforcement mechanisms.
[571] TRIPS, supra fn. 282.
[572] CDPA 1988, supra fn. 304.
[573] [1974] A.C. 819.

Dilhorne described it as an "agreement by two or more by dishonesty to deprive a person of something which is his or to which he is or would be or might be entitled and an agreement by two or more by dishonesty to injure some proprietary right of his".[574] The highest available penalty for this offence is 10 years of imprisonment and/or an unlimited fine.

The earlier mentioned case of *R v Allan Ellis* (2010)[575] can serve here as the first example of the use of conspiracy to defraud against a relevant online intermediary. he defendant in those proceedings operated a BitTorrent-oriented music sharing website known as Oink's Pink Palace. In 2007, using the charges of conspiracy to defraud, the British police arrested the website's operators and Oink's servers (located in the Netherlands) were seized. The Middlesborough Crown Court found the defendant operators to have acted dishonestly and refused to apply the E-Commerce Directive's safe harbour;[576] however, the jury acquitted the defendants. Nevertheless, this case stands (among others) as a testimony to the reach of criminal liability applied in the discussed context; reliance on this type of liability enables the use of, for example, the cross-border enforcement measures (such as the seizure of servers), and organisations representing the copyrightholders are more than keen to further facilitate the use of such mechanisms.

The second case covered in this section, which also involved charges of conspiracy to defraud being pressed against online intermediaries, is *R v Rock and Overton* (2010).[577] The website which was at the centre of those proceedings, TV Links, initially provided links to videos hosted by third-party websites such as Megavideo, a sub-platform of the late Megaupload. Later on, it developed its own streaming web-player, used for viewing the content from the same third-party websites directly. Unsurprisingly, a significant amount of videos to which TV Links facilitated the access to was infringing copyright.

[574] *Scott v Commissioner*, supra fn. 573, at 840.
[575] *R v Allan Ellis*, supra fn. 113 and section 2.2.3.1 of chapter one.
[576] The safe harbour provisions of the E-Commerce Directive are discussed below, in section 3.3.1 of the current chapter.
[577] *R v Rock and Overton*, supra fn. 90.

As a result, the owner and operator of this website was arrested in October 2007, following an investigation conducted by the Federation Against Copyright Theft (a private body, hereafter referred to as FACT) and the Gloucestershire Police. At the same time, the website's servers were seized (also) in the Netherlands, where BREIN (Dutch agency, equivalent of FACT) served a relevant notice to the TV Links' hosting provider.

The initial charges relied on at the time of the arrest were criminal copyright infringement (in the form set in s. 107 (2A)[578]) and conspiracy to defraud. However, during the trial, the prosecution focused solely on the latter offence. This has proven to be unsuccessful – the judge found that the operator of TV Links is protected by reg. 17 of the E-Commerce Regulations 2002 (implementing art. 12 of the E-Commerce Directive[579]).[580]

Despite the fact that the operator of TV Links was acquitted, the website did not go back online. In an interview with torrentfreak.com, the operator stated that following the trial he no longer had the will to maintain TV Links, especially given the fact that a replacement website (tvlinks.ws) began to function shortly after his website was taken down.[581]

The third case (or rather an incident) discussed in this part of the subchapter occurred in relation to one of the oldest BitTorrent websites, which was known as Filesoup. Between 2003 and 2005, it acted as a BitTorrent tracker, but after 2005, it became a forum where users could exchange links to BitTorrent files. Needless to say, a significant amount of files shared through Filesoup was copyright-infringing.

---

[578] CDPA 1988, supra fn. 304.
[579] The safe harbour provisions of the E-Commerce Directive are discussed in section 3.3.1 of the current chapter.
[580] *R v Rock and Overton*, supra fn. 90.
[581] See http://torrentfreak.com/busted-tv-show-site-in-limbo-as-authorities-back-off-081121/

In 2009, the operators of Filesoup were arrested, and their website was taken down through the seizure of their computer equipment.[582] They were initially charged with conspiracy to defraud, but interestingly enough, the Crown Prosecution Service (CPS) dropped its charges in 2011, stating that it was "neither necessary nor appropriate to continue to pursue this matter in a criminal court".[583] In the end, this decision did not bring the website back to cyberspace. A continuous exodus of its users (which occurred after the arrests) led to the website's closure in June 2012.[584]

The last incident to be covered in this section (which provides for a rather unconventional development in this area of law) is the case of the earlier mentioned Surf The Channel website,[585] which was a video search engine, hosting links to (often infringing) content hosted on third-party websites. Following an undercover investigation by FACT (which involved accessing the defendants' house), the operators of Surf The Channel were charged with conspiracy to defraud, arrested, and their computer equipment was seized.[586]

Just as in the case of Filesoup, CPS decided to drop its charges, before the start of the "official" criminal prosecution.[587] However, this is where the case took a different direction. FACT decided to bring a private prosecution, and for that purpose the US-based programmer who coded for Surf The Channel was charged by the US authorities with conspiracy to commit copyright infringement.[588] He was, however, offered a deal – the charges against him would be dropped if he testified in the UK trial against his former employers.

---

[582] See http://www.guardian.co.uk/technology/2009/aug/04/file-soup-sharing-tv-movies
[583] See http://the1709blog.blogspot.co.uk/2011/02/parasites-in-filesoup.html
[584] See http://torrentfreak.com/worlds-oldest-bittorrent-site-shuts-down-120605/
[585] Surf The Channel case, supra fn. 94.
[586] See http://torrentfreak.com/undercover-mpaa-agents-expose-alleged-movie-pirates-120521/
[587] Supra fn. 586.
[588] See http://www.fbi.gov/boston/press-releases/2011/former-milford-man-charged-with-conspiracy-to-commit-copyright-infringement

The programmer agreed, and in June 2012 the Newcastle Crown Court found the operator of Surf The Channel guilty of conspiracy to defraud.[589]

3.2.2. Criminal copyright infringement.

At the time of writing, the earlier mentioned offence set out in s. 107(2A) of the CDPA 1988 has not produced any noticeable legal decisions in which online intermediaries' liability would be discussed. However, in June 2013, the British police began targeting various filesharing websites with letters of the following substance:

> "We have grounds to suspect that as owners and/or operators of the XXXXX website, you are committing the offence of communication to the public under s.107(2A) of the Copyright, Designs and Patents Act 1988 ("CDPA"). Section 107(2A) is an indictable offence punishable by up to two years' imprisonment (…)"[590]

Moreover, the notice is further reinforced by the mention of the Serious Crime Act 2007, s. 44(1)(A) of which states that "a person commits an offence if (…) he does an act capable of encouraging or assisting the commission of an offence; and (…) he intends to encourage or assist its commission".[591] This indicates that, apart from s. 107(2A), the relevant online intermediaries could be placed under criminal liability for encouraging or assisting their users in committing the offences set in s.107.[592]

The letters ask the operators wishing to avoid liability for the described offences to make contact with the National Fraud Intelligence Bureau unit of

[589] See http://torrentfreak.com/surfthechannel-owner-found-guilty-of-conspiracy-to-defraud-120627/
[590] See http://torrentfreak.com/uk-police-launch-campaign-to-shut-down-torrent-sites-130604/
[591] Serious Crime Act 2007 c. 27, s. 44(1)(a).
[592] The said offences are set out in section 2.2 of this chapter.

the City of London police (hereafter referred to as the NFIB).[593] For the moment, we have yet to see whether those who refrain from doing so are going to be actually charged, and whether the courts are going to find such unresponsive operators liable for the offences in question.

3.3. Limitations on intermediary liability.

At the end of the 1990s, it started to become clear that due to the infringing activities of their users, many online intermediaries were facing the prospect of tremendous amounts of liability, which - if left without appropriate floodgates - could carry a very large burden with them. In her 2009 article from 2009, Edwards presented three arguments for why imposing such a burden could be perceived as inappropriate: firstly, intermediaries often have a limited amount of practical and legal control over the content shared through their services. Secondly, such an approach could be perceived as unjust. And thirdly, the said approach could potentially cause a chilling effect on the development of this sector of technological services.[594] Perhaps consequently to those factors, some of the key lawmakers around the world introduced legislative measures aimed at limiting the liability of online intermediaries for infringing acts of their users; in US, the said measures were introduced through the Digital Millennium Copyright Act 1998, and in the EU, through the E-Commerce Directive[595] (referred to in this part of the thesis as "the Directive"). This section, as it could be predicted, focuses on the mechanisms implemented by the latter, with attention given primarily to the "safe harbours" set in articles 12, 13 and 14, and the "no obligation to monitor" provision dwelling in art. 15 of the Directive.

3.3.1. The E-Commerce Directive's "safe harbours".

[593] Supra fn. 590.
[594] Edwards L, 'The Fall and Rise of Intermediary Liability Online' in Edwards L and Waelde C (eds), *Law and Internet* (Hart 2009), 47, at 59.
[595] E-Commerce Directive, supra fn. 91.

3.3.1.1. Description of the provisions.

According to art. 2 of the Directive, the three "safe harbours" apply to entities providing an "information society service", the term further defined in Directive 98/34 as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".[596] It is worth adding that despite being mentioned, provision of services for remuneration is *not* a requirement which has to be fulfilled by an entity to qualify as underlined in, for example, the earlier mentioned case of *Davison v Habeeb*.[597]

The first of the three harbours, set out in art. 12 of the Directive, is often referred to as the "mere conduit" harbour and is the most geared towards connection-providing ISPs. It states that:

- "(w)here an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted (…)"[598]

That being said, the service provider is only going to be shielded from liability if it "does not initiate the transmission;"[599] "does not select the receiver of the transmission;"[600] as well as "does not select or modify the information

[596] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services (as amended by the 98/48/EC Directive), art. 1(2).
[597] *Davison v Habeeb*, supra fn. 221, at 54.
[598] E-Commerce Directive, supra fn. 91, art. 12.
[599] E-Commerce Directive, supra fn. 91, art. 12(1)(a).
[600] E-Commerce Directive, supra fn. 91, art. 12(1)(b).

contained in the transmission".[601]

Article 13 of the Directive sets out the second harbour, which could be referred to as the "caching" harbour. It states that those Information Society Service Providers (referred to as the ISSPs) whose services consist of "the transmission in a communication network of information provided by a recipient of the service"[602] are to be excluded from liability for "the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request".[603] However, as in art. 12, certain conditions have to be met in order for an ISSP to qualify for this harbour. It has to be confirmed that:

- "(a) the provider does not modify the information;
- (b) the provider complies with conditions on access to the information;
- (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
- (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
- (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement".[604]

While it is certainly an important provision in the law's struggle to keep up with the digital age, it should be noted that art. 13 does not really affect the

[601] E-Commerce Directive, supra fn. 91, art. 12(1)(c).
[602] E-Commerce Directive, supra fn. 91, art. 13.
[603] E-Commerce Directive, supra fn. 91, art. 13.
[604] E-Commerce Directive, supra fn. 91, arts. 13(1)(a) to 13(1)(e).

enforcement schemes aimed at the removal of access to infringing content.

The third and last safe harbour, focused on the providers of "hosting" services, is arguably the one which has proven to be the most controversial. It is implemented by art. 14 of the Directive, and states that:

- "Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service; (…)".[605]

Yet again, the exclusion from liability is not unconditional. The ISSPs cannot possess the "actual knowledge of illegal activity or information",[606] and, as far as claims for damages are concerned, the ISSP cannot be "aware of facts or circumstances from which the illegal activity or information is apparent".[607] Alternatively, should such knowledge or awareness be acquired, the service provider must act "expeditiously"[608] to "remove or to disable access to the information".[609]

It is worth adding that all three "harbour" articles contain provisions reserving the right for Member States' authorities to require the ISSPs to "terminate or prevent an infringement".[610] Moreover, art. 14(3) states that the liability limitation described therein does not "affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information".[611]

3.3.1.2. Judicial interpretation of the E-Commerce Directive safe harbours.

[605] E-Commerce Directive, supra fn. 91, art. 14.
[606] E-Commerce Directive, supra fn. 91, art. 14(1)(a).
[607] E-Commerce Directive, supra fn. 91, art. 14(1)(a).
[608] E-Commerce Directive, supra fn. 91, art. 14(1)(b).
[609] E-Commerce Directive, supra fn. 91, art. 14(1)(b).
[610] E-Commerce Directive, supra fn. 91, arts. 12(3), 13(2) and 14(3).
[611] E-Commerce Directive, supra fn. 91, art. 14(3).

As mentioned in the previous section, art. 14 has arguably attracted the most attention out of the three; and it is especially the case within the area of infringing activities lying at the centre of this thesis. Hence, this subsection is going to focus on providing an insight into the European Union's courts' interpretations of the key aspects of the "hosting" safe harbour.

The first interpretative challenge which the courts have to face is to decide whether a certain type/service model of an online intermediary comes under the definition of a "hosting provider". For example, in the earlier mentioned case of *Netlog*, the CJEU had to consider whether a social media website fulfils this criteria: the judges answered this query positively, stating that "it is not in dispute that the owner of an online social networking platform (…) stores information provided by the users of that platform, relating to their profile, on its servers, and that it is thus a hosting service provider within the meaning of Article 14".[612]

This was, however, rather a fairly straightforward matter to decide on. Things get much more difficult when we arrive at further requirements related to the online intermediary's service model. For example, in the case of *Google v Louis Vuitton* (2010), the CJEU held that, in order to qualify for art. 14, an intermediary has to play a role which is "neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores".[613] Following this trail, the CJEU proclaimed in *L'Oréal v eBay* that art. 14 protects online marketplace operators who do not play an "active" role in the transfer of information: a given example of an activity placing such ISSPs in that role was providing assistance through, for example, optimising the presentation of offers for sale and promoting them.[614]

[612] *SABAM v Netlog*, supra fn. 103, at [27].
[613] Case C-236/08 *Google France SARL v Louis Vuitton Malletier SA* [2010], at [114].
[614] *L'Oréal v eBay* (CJEU), supra fn. 165, at [116].

One might wonder, what is the purpose of the "passive role" requirements described in the preceding paragraph? The answer to this question is directly related to the actual and constructive knowledge elements of art. 14. The less control of/interaction with the content an ISSPs has (ie. the more passive role it plays), the lower the chance of proving that it was "aware of facts or circumstances from which the illegal activity or information (was) apparent".[615] In order to add some clarity to the "hosting" harbour, the CJEU sought to establish certain characteristics of ISSPs which would be influencing the finding of the said awareness – though it is questionable whether they succeeded in this endeavour.[616]

At times, proving actual knowledge of infringing activities is a relatively straight-forward exercise – example being the Swedish case of The Pirate Bay (hereafter referred to as TPB).[617] While the court found TPB to be a hosting provider within the meaning of art. 14, the finding of actual knowledge was not difficult with TPB operators openly ridiculing the notice and takedown letters on their front page.[618] Since TPB certainly did not "act expeditiously" to remove access to the infringing information, the website's operators were not able to benefit from this liability exemption. In other, less clear-cut, cases the judges often turned to using aspects of ISSPs' services as indicators of the existence of the constructive knowledge element. For example, in the earlier mentioned UK defamation case of *Kaschke v Gray* it was held that checking the spelling and grammar of user-generated content triggers the finding of facts and circumstances from which the existence of infringing content should have been inferred.[619] The decision in *L'Oréal v eBay* also contained more specific guidance with regards to the mental element of art.14. It introduced the idea of looking at the ISSP as the "diligent economic operator",[620] this being an objective element of the test for knowledge of the infringing activity resulting from being aware of relevant facts or circumstances.

[615] E-Commerce Directive, supra fn. 91, art. 14(1)(a).
[616] See section 2.4.1 of chapter five.
[617] The Pirate Bay trial, supra fn. 111.
[618] Supra fn. 111.
[619] *Kaschke v* Gray, supra fn. 224, at [86].
[620] *L'Oréal v eBay* (CJEU), supra fn. 165, at [120].

The CJEU in *L'Oréal* also underlined the significance of the infringement notices filed by the rightholders as a key factor that the Member States' courts should take into account when deciding on the existence of facts indicating actual or constructive knowledge of the illicit activities.[621] That said, the judges recognised that a notice of this kind does not necessarily trigger the finding of the mental state in question, since the said notice "may turn out to be insufficiently precise or inadequately substantiated".[622] In fact this is quite a problematic aspect of art. 14 – especially when we consider, for example, the area of defamatory content, where it might be fairly difficult for the online intermediaries to decide whether an infringement notice is aimed at actually infringing content. This issue was present in the earlier mentioned case of *Davison v Habeeb*, where it was held that Google (as the operator of Blogger) did not acquire actual or constructive knowledge since it "was faced with conflicting claims from the claimant and the second defendant between which it was in no position to adjudicate".[623]

Moving on to article 12 and the "mere conduit" harbour. It did not bring as many complex interpretative problems as art. 14, but it is still worth mentioning two UK cases where the former provision was called in by the online intermediaries.

Firstly, the earlier mentioned case of *R v Allan Ellis*[624] featured an attempt to rely on the "mere conduit" harbour in order to defy the charges of conspiracy to defraud. However, the judge denied this attempt on a rather interesting basis; he held that art. 12 is aimed at principally legitimate operations, and Oink's Pink Palace (the defendant's website) did not count as such.[625] Such reasoning (while holding a certain amount of appeal) raises difficult questions,

[621] *L'Oréal v eBay* (CJEU), supra fn. 165, at [122].
[622] *L'Oréal v eBay* (CJEU), supra fn. 165, at [122].
[623] *Davison v Habeeb*, supra fn. 221, at [68].
[624] *R v Allan Ellis*, supra fn. 93.
[625] *R v Allan Ellis*, supra fn. 93, at [8].

for, arguably, none of the online intermediaries presented on the preceding pages can be regarded as illegitimate *per se*. It is mainly the *use* of those intermediaries' services which makes them "legitimate" or not. It is not, however, clear on how we should assess the overall legitimacy of an online service. Should we use percentages, and regard a website used in 51 % for infringing activities as illegitimate, leaving a website used for the same activities in 49 % as legitimate? Perhaps embracing this question is not the best solution, and a different approach should be explored.[626]

Secondly, in the earlier mentioned case of *R v Rock and Overton* the judge initially considered TV Links to lie outside of the "mere conduit" exception, since he saw the operators as assisting their users in infringing activities: and recital 44 of the E-Commerce Directive states that "a service provider who deliberately collaborates with one of the recipients of his service in order to undertake illegal acts goes beyond the activities of 'mere conduit' or 'caching' and as a result cannot benefit from the liability exemptions established for these activities".[627] However, the defendants were ultimately able to rely on art. 12, since the E-Commerce Regulations (implementing the E-Commerce Directive into the English law) did not transpose rec. 44 into the UK law.[628]

Overall, it seems plausible to agree with Edwards, who wrote that the EU safe harbour regimes are "bending and breaking" under the courts' attempts to get around them,[629] cases of *L'Oréal*, *Kaschke* and *Allan Ellis* supporting this position. Similarly, Savola submits that "in practice, courts have found ways to find platform providers liable owing to awareness, participation or some other basis. This has also led to undesirable uncertainty as to what exactly could cause liability for platform providers".[630] The situation is even more problematic, given that it is often uncertain where the bended line actually is:

[626] For example, the one proposed in chapter five of this thesis.
[627] Electronic Commerce (EC Directive) Regulations 2002, rec. 44.
[628] *R v Rock and Overton*, supra fn. 90.
[629] Edwards, supra fn. 594, at 84.
[630] Savola, supra fn. 401, at 285. For further discussion of the legal certainty problem, see section 2.2 of chapter five.

the difficulties related to the mental element of art. 14 being a testimony to this perception. Valgaeren and Roland also wrote in this vein, stating in relation to the safe harbour case law that "reading these judgments, one cannot help but observe that the courts (too) appear to be groping with the law".[631] They have added that oftentimes, the judges begin from the conviction that operators are liable (especially where the latter derive profits from facilitating the infringing activities of their user), and then try to find legal backing for this position.[632] Such an attitude could be, to an extent, understood (though not necessarily recommended) in cases involving, for example, filesharing websites used for tremendous amounts of copyright infringement or revenge pornography websites. Last but not least, it should be noted that it is very probable that the "expeditious removal" requirement of art. 14 incited the development of many N&T schemes[633] amongst the online intermediaries.

3.3.2. Article 15 and "no obligation to monitor".

In addition to the "safe harbour" provisions of articles 12, 13 and 14, article 15 introduced an additional layer of protection for online intermediaries whose services are used for infringing purposes. It states that:

- "Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity".[634]

The discussion of this provision conducted in section 3.1.2.2 of the current chapter can be complemented by the following points. In *L'Oréal v eBay*,

[631] Valgaeren E and Roland N, 'Youtube and social networking sites – new kids on the block?', in Strowel A and Triaille J-P (eds), *Google et les nouveaux services en ligne* (2008), at 224.
[632] Valgaeren and Roland, supra fn. 631, at 224.
[633] Described above, in section 3.1.2.1 of the current chapter.
[634] E-Commerce Directive, supra fn. 91, art. 15(1).

despite the support given to the prevention of infringements, art.15 appeared in the judges' reasoning when they held that "the measures required of the online service provider concerned cannot consist in an active monitoring of all the data of each of its customers in order to prevent any future infringement of intellectual property rights".[635] And in the earlier mentioned case of *Scarlet Extended v SABAM*, the CJEU stated that the demanded network filtering system (described above[636]) "would be contrary to art.15(1) E-Commerce Directive",[637] for it would entail "monitoring all data from all customers for any future infringement of intellectual property, for an unlimited time".[638] That said, as Kulk and Zuiderveen rightly note, the judgment provided little guidance on how art. 15 would be applied to more specific (and balanced) preventive filtering schemes.[639] According to Ginsburg, a legal provision of this kind should not entitle the service provider to remain "militantly ignorant" of the illicit activities occurring on its network,[640] and, following this line of thought, we might see, for example, carefully tailored filtering schemes being considered as a part of the solution to the problem (for example, the earlier mentioned *GEMA v Rapidshare*[641] case).

Finally, it is worth remarking upon the potentially troubling connection between art. 15 and the provisions of articles 12 to 14 reserving the possibility for Member States to introduce measures requiring the ISSPs to "terminate or prevent an infringement". In practice, preventing infringements in cyberspace almost instantly evokes the concept of filtering schemes, together with the notion of searching for "facts or circumstances indicating illegal activity". Hence, there is plenty of room for conflict and legal uncertainty in this regard.

---

635 *L'Oreal v eBay* (CJEU), supra fn. 165, at [139].
636 In section 3.1.2.3.1 of the current chapter.
637 *Scarlet Extended v SABAM*, supra fn. 105, at [40].
638 *Scarlet Extended v SABAM*, supra fn. 105, at [40].
639 Kulk and Zuiderveen, supra fn. 363, at 794.
640 Ginsburg, supra fn. 473, at 238.
641 *GEMA v Rapidshare*, supra fn. 496; though the degree to which the injunction granted in this case was "carefully tailored" is rather questionable.

Chapter 3 – Enforcement schemes' effectiveness.

1. Introduction

Having covered the scenarios through which infringing content is shared in cyberspace (chapter one), as well as having described the enforcement schemes employed to remove access to such content (chapter two), this thesis may now proceed to the first of its evaluative chapters, one focused on the effectiveness of the presented enforcement schemes. It is difficult to deny that regardless of the content type, the endorsed enforcement mechanisms should be meeting this aim in practice, not just in theory. The notion underlined in art. 8(1) of the InfoSoc Directive with regards to the remedies provided for therein ("the sanctions provided in respect of the rights and obligations protected by this directive are to be "*effective*, proportionate and *dissuasive*),[642] applies across all four covered content types. Accordingly, as Lodder and Meulen noted, "symbolic" or insignificantly effective measures should not be endorsed.[643]

Also, just as when one thinks about a car: the preliminary, crucial question should be whether it performs its primary function, that is driving – after this can (and should) come the questions about the car's safety, CO2 emissions or aesthetics.[644] Tasks such as assessing the enforcement schemes' compatibility

[642] Information Society Directive, supra fn. 8, art. 8(1); emphasis added. The word "dissuasive" was also highlighted because it forms here, in this author's opinion, a key part of the word "effective".

[643] Lodder A and Meulen N, 'Discussion of the Dutch Pirate Bay Case Law and Introducing Principles on Directness, Effectiveness, Costs, Relevance and Time' (2012) JIPITEC 4(2), 130, at 138.

[644] Of course, if the negative side effects of driving a specific car/running a specific enforcement scheme outweigh the benefits coming from the performance of the said items, the car should not be allowed on the road, and the enforcement scheme should not be endorsed by the legal system; see section 2.3 of chapter five.

with human rights are without doubt vital in this area of research, but it makes sense to perform them after the current chapter.[645]

Attempting to precisely evaluate the effectiveness of a legal enforcement mechanism is often a considerably difficult task, especially within the realm of online regulation – as the following chapter is going to demonstrate. Evidence of successful removal of access to infringing content is notoriously difficult to obtain; that said, there are several categories of data which, despite their relative scarcity, might be of use in this part of the thesis.

Firstly, a researcher might seek the data about the availability of infringing content directly; for example, if, despite a series of notice and takedown submissions, the targeted infringing content can be located and accessed by the researcher, the lack of effectiveness is fairly clear. Similarly, if a researcher is able to access the supposedly blocked "infringing" website, with or without the use of circumvention measures, a parallel conclusion might be reached. The online setting of the discussed challenges also allows for the reliance on certain forms of the Internet traffic data – for example, researchers might wish to observe the BitTorrent traffic before and after the implementation of enforcement schemes such as graduated response or website-blocking aimed at services running torrent trackers. This kind of data might be seen as holding an advantage over availability-focused information, for the former might be more likely to show whether infringing content is actually being spread or not. Survey-based empirical research might also play a role here – for example, online users might be asked about their perception of a specific enforcement scheme, for example whether the prospect of being subjected to criminal penalties deters them from sharing infringing content, whether they rely on circumvention measures etc.

[645] See chapters four and five.

In the realm of copyright-infringing content (as well as that infringing trademarks), it is also possible – and quite adequate – to look at the impact of the employed enforcement schemes on the sales of the legitimate versions of the infringed content. As Danaher and Smith rightly noted, simple prevention of infringing activity in instances where, for example, the infringer would not have watched the copyrighted movie if it was not for the pirate resources, feels insufficient[646] – while such a prevention might stop the potential "domino effect" of infringement within the society,[647] in most cases, successful enforcement schemes aimed at copyright- or trademark- infringing content should bring about an increase in the profits coming from the original, legitimate goods.[648] The unfortunate challenge in obtaining data proving this is quite clear –it is exceedingly difficult to precisely attribute an increase or a decrease of profits to a specific measure. That is not to say that attempts to gather this information have not been made or that such data is of no use in this segment of the thesis – it simply means that it cannot be regarded as an infallible measurement of effectiveness.

The following chapter relies on a variety of research perspectives and empirical data types described in the preceding paragraphs, in order to uncover as many "road signs" leading to an improvement in the effectiveness of this branch of online enforcement policy as possible. It has to be stated that this search is challenged by the general scarcity of the earlier mentioned empirical data – for example, while a fair amount of studies was conducted with respect to the impact of online piracy on the copyright owners' interests,[649] it is considerably more difficult to find studies assessing the effectiveness of the enforcement schemes aimed at the said phenomenon. Furthermore, while copyright-infringing content already plays a prevalent role in this thesis, the empirical research relevant to this chapter pushes this inequality even further;

[646] Danaher B and Smith M,'Gone in 60 Seconds: The Impact of the Megaupload Shutdown on Movie Sales (2013) (available at SSRN: http://ssrn.com/abstract=2229349), at 3.
[647] On which see section 3.1 of the current chapter.
[648] Danaher and Smith, supra fn. 646.
[649] See, for example, Liebowitz S, 'Will MP3 downloads annihilate the record industry? The evidence so far' in Libecap G (ed),*Intellectual Property and Entrepreneurship* (2004) or Zentner A, "File sharing and international sales of copyrighted music: An empirical analysis with a panel of countries"(2005) Topics in Economic Analysis & Policy 5(1).

it is extremely rare to find an effectiveness-oriented study focused on privacy-infringing or defamatory content, with trademark-infringing content being at a similar disadvantage.

Nevertheless, it is difficult to deny that the questions lying at the heart of this chapter desperately need answers – and for the moment, it is feasible to rely on the available (though imperfect) data to see whether it might shed some light on the currently endorsed enforcement schemes' effectiveness.

To this end, the chapter adopts the following analytical structure. Firstly, subchapter 2 discusses the primary, "first tier" challenges which can be seen as impairing the effectiveness of enforcement schemes presented in chapter two. This includes the problem of infringing content returning to the platform/service which was targeted by the enforcement scheme (section 2.1), the phenomenon of users' migration to alternative sources of infringing content (section 2.2), as well as the issue of circumvention of the enforcement schemes' technological components (2.3). Understanding those challenges and retaining them in mind is the first, fundamental part of effective policymaking in this area of law. Building upon its predecessor, subchapter three assesses the deterrence effect of the endorsed enforcement schemes, which can be seen as one of the key desired results of the said schemes' operation. Subchapter four explores the issue of diminishing returns – it is crucial for the rightholders and governments vesting their resources in specific enforcement schemes to be confident that it is worth doing so, that the actual removal of access to infringing content matches the costs of running the said enforcement measures. Finally, subchapter five focuses on a slightly broader dimension of the discussed struggle for effectiveness, that is on the phenomenon of the modern day society's prevalent acceptance of infringing content.

2. Primary areas of concern.

2.1. Renewal of access to infringing content (on a single platform).

The first challenge discussed in this section of the chapter is almost an obvious, preliminary one. Whenever an enforcement scheme seeks to remove access to a piece of infringing content on a specific platform, it often turns out that such content returned to the same service in one form or another. The following paragraphs are going to discuss the scenarios which might lead to such "resurrection" of infringing content, by reference to the specific enforcement schemes which are affected by this challenge.

The notice and takedown procedure[650] (together with specific content removal injunctions) is probably the main enforcement scheme which is troubled by the issue of infringing content returning, for example, onto the same website from which the rightholders wished to erase it. In copyright, this occurs when, for example, a cyberlocker like Rapidshare receives a notice of infringement and removes the file complained of; however, shortly afterwards, the file is reuploaded again, either by the same user or a different one. The likelihood of such a return is augmented by the fact that it is often a practice among the regular uploaders of infringing content or editors of indexing websites to verify periodically whether the content in question is still available (ie. whether it has been taken down or not). In the field of trademarks, infringing information might return to the platform of origin when, for example, a company like L'Oréal notifies eBay about the counterfeit offers infringing L'Oréal's trademark, eBay removes the offers from its website; but soon after, the seller uploads it again, or other counterfeit sellers fill in the gap and upload the same infringing offer. Privacy-infringing or defamatory content placed within, for example, a blog post on Blogger, might be taken down following a notice of infringement, but return onto the platform shortly afterwards, either on the same blog or on another blog hosted on the website in question.

[650] Described above, in section 3.1.2.1 of chapter two.

A study conducted by Lauinger et al in 2013[651] within the area of copyright shows just how prevalent the problem of the "revival" of infringing content might be to the notice and takedown and similar schemes. By collecting and analysing the data on the lifetime of a set of links leading to infringing content uploaded to over twenty one-click-hosting websites, the researchers conducting the study found out that on most cyberlockers, more than 50 % of the infringing files remained online for more than a month and concluded that "takedown notices might be responsible for only a fraction of pirated files becoming unavailable".[652] The key reason for the latter finding was that there are so many mirror files (copies of a single file) being uploaded, that the "current levels of takedown requests fail to render content unavailable".[653]

It is also worth adding that the accounts of infringing users exhibit a similar, "reappearing" tendency as the infringing content does. Notices of infringement aimed at the accounts of forums', cyberlockers', auction websites' (etc.) users might have a certain impact, as far as consumer trust (primarily in the case of auction websites) or online personality (for example, in case of forums or blogs) go, but in the end replacement accounts are often likely to appear again. Though it is probably more difficult to regain a good seller's standing on an auction website than it is to re-establish one's identity on a forum[654] or uploader's profile on a cyberlocker website.

It should be added that content removal measures aimed at indexing services (which are merely linking the users to infringing content, without hosting the content itself) are facing the discussed challenge as well, to an augmented extent - reuploading a link to a piece of infringing content is generally much quicker than reuploading the content itself.

---

[651] Lauinger T and others, 'Clickonomics: Determining the Effect of Anti-Piracy Measures for One-Click Hosting' (2013), available at http://tobias.lauinger.name/#publications
[652] Lauinger et al, supra fn. 651, at 11.
[653] Lauinger et al, supra fn. 651, at 11.
[654] That being said, in a situation where the banned users' posts are deleted, it might be difficult to regain the forum identity nonetheless.

Of course, the recurring game of 'whack-a-mole' described in the preceding paragraphs did not go unnoticed and many rightholders turned towards preventive filtering schemes, just as described earlier.[655] While it is likely that some of them turned out to be fairly effective (Youtube's Content ID probably being the main example here), such enforcement schemes became impaired by two principal factors. First of all, it is oftentimes rather difficult to persuade/force the intermediaries to implement forms of preventive filtering on their services: as shown above[656] in the discussion of art. 15 of the E-Commerce Directive[657] and of cases such as *Scarlet Extended*.[658] Secondly, such filters are often vulnerable to being circumvented, like the enforcement schemes analysed in section 2.3 of the current chapter. Uploaders might reupload the same files under different names,[659] change the elements of the files used by the filtering system, etc.

Additionally, it is also worth giving attention here to one of the ways in which infringer-focused enforcement schemes such as graduated response or civil liability in damages are affected by the issue of infringing content reappearing on the same platform. Let us take graduated response and its impact on the BitTorrent-based copyright-infringing filesharing as an example: while a recipient of a warning letter(s) might decide to cease his activities, the content he uploaded onto the network might be already seeded (ie. made available) by others – a concern affecting multiple infringer-focused measures. The same applies to an infringer who, for example, uploaded privacy-infringing pictures onto a revenge pornography website like IsAnybodyDown;[660] while he might become liable in damages to the rightholder and remove his infringing uploads, the pictures themselves might be already on other users' hard drives, and those users might continue reuploading them onto the same website despite the original poster ceasing his activity. Collingwood referred to this difficulty when discussing injunctions aimed at restraining the publication of

[655] See section 3.1.2.2 of chapter two.
[656] See sections 3.1.2.2 and 3.3.2 of chapter two.
[657] E-Commerce Directive, supra fn. 91, art. 15.
[658] *Scarlet Extended v SABAM*, supra fn. 105.
[659] See the discussion of the *Atari v Rapidshare* case covered in section 3.1.2.2 of chapter two.
[660] See section 4.2.1 of chapter one.

privacy-infringing content (such as the order granted in the *CTB v News Group Newspapers*[661]). She stated that, while in the offline world they "may well be the primary remedy or, indeed, the only effective remedy in respect of privacy violation, the same cannot be said in respect of the on-line environment, where publication is instantaneous and often distributed to a very wide audience".[662] Within this line of concern, applicable to both the current and the following section, privacy-infringing content seems to be the most affected out of the four content types covered in this thesis.

2.2. Movements towards the alternative sources of infringing content.

Whilst an extremely sophisticated filtering scheme could (theoretically) prevent infringing content from appearing on, for example, a website which endorses it, and a complex, circumvention-proof[663] ISP blockade could prevent the EU citizens from accessing a website used for illicit purposes, if infringing content was to appear exclusively on a single online platform, this thesis would probably be no more than a thirtieth of its length. As it is undoubtedly clear after many years of the enforcement struggle, this area of lawmaking is exceedingly challenging because of the ever-increasing amount and variety of platforms used for infringing purposes. The infringing information has a tendency to continuously travel from one service to another and should one source of, for example, copyright-infringing content "dry up" following a successful application of the enforcement measures, the users seeking such content might float to another online source and satisfy their thirst there. It is this migration of online users between various sources of infringing content which is the subject of this section (in contrast to the issue of such content returning onto the same platform, a challenge covered in the preceding section). It should be noted that the notion of migration is

[661] *CTB v News Group*, supra fn. 200.
[662] Collingwood, supra fn. 245, at 5.
[663] (Note – does not exist.)

interpreted in a fairly broad sense; for example, the term also covers situations where users "stumble" upon the infringing content on an alternative service, without actively looking for such information.[664]

The primary enforcement schemes whose effectiveness is challenged by the users' migration to alternative sources of infringing content (hereafter referred to as the "altsources migration") are the schemes focused on removing access to an online service used for infringing purposes. The first of them to be covered in the following paragraphs is the usage of criminal law measures aimed at disabling the "infringing" service's capability to operate.[665] Among such efforts, it is difficult to find a case as far-reaching and widely discussed as the Megaupload takedown. While this is not an EU case, the shutdown of this cyberlocker by the US Department of Justice had a considerable impact on the filesharing ecosystem and produced empirical data which can be relied on for the purposes of this chapter.

First of all, the factual circumstances of the takedown mentioned in chapter one[666] deserve to be elaborated on. On the 19th of January 2012, the owners and operators of Megaupload (at the time, one of the biggest cyberlockers in cyberspace) were arrested on (inter alia) the charges of criminal copyright infringement, while their servers were seized by the federal government of the United States. Subsequently, Megaupload disappeared from the Internet. Now that the dust has settled, it is possible to consider how effective this step was in reducing the levels of ongoing online piracy and - specifically for this section– whether the altsources migration could be observed after the takedown (and, assuming a positive answer, on what scale).

[664] This could particularly be the case within the domain of privacy-infringing and defamatory content.
[665] See section 3.2 of chapter two.
[666] See section 2.2.1 of chapter one.

It is confirmed that the Megaupload incident had at least some impact on the operators of other filesharing services. In the days following the arrests, Filesonic and Fileserve (both of them being popular cyberlockers) have gone into a "no-sharing" mode[667] – allowing users to access their own files, but preventing them from being downloaded by anyone else.[668] Additionally, Uploaded.to (another cyberlocker) banned connection requests from all US-based IP addresses.[669] On top of this, two video streaming services, VideoBB and VideoZer, closed their affiliate programmes (rewarding the users who uploaded files which were viewed most often – as one might predict, these often consisted of illegally uploaded copyrighted material).[670]

Furthermore, the HADOPI agency, eager to affirm the effectiveness of taking down Megaupload, reported on a data set indicating that the users of this cyberlocker moved to legitimate services upon its downfall.[671] Using Mediametrie/NetRatings (both of them are media audience measurement companies) data gathered in January 2012, the report shows an increase from 748,000 to 941,000 daily clicks registered on legitimate video-on-demand (VOD), TV-catch up, and aggregator services, with VOD services registering a 35 % increase in popularity. This last piece of data is particularly valuable, since Megavideo (the video streaming component of Megaupload) was an extremely popular website in France.[672] The positive impact of the shutdown on the income of the legitimate rightholders is further indicated by a study conducted by Danaher and Smith in 2013, which found that "the shutdown of Megaupload and its associated sites caused digital revenues for three major

---

667 See http://torrentfreak.com/cyberlocker-ecosystem-shocked-as-big-players-take-drastic-action-120123

668 As a result, Filesonic went offline later on - http://www.bbc.co.uk/news/technology-19437148

669 See http://torrentfreak.com/uploaded-to-blocks-us-visitors-120121/

670 Supra fn. 667. For the introduction to reward programmes and cyberlocker mechanics in general, see section 2.2.1 of chapter one.

671 *Note d' information: Analyse de l'impact de la fermeture de MegaUpload :+25,7% d'audience pour les plateformes de Catch-Up TV et de VOD, HADOPI* (2012), available (in French) at: http://www.hadopi.fr/sites/default/files/page/pdf/Note_Fermeture_Megaupload.pdf

672 See http://www.mediametrie.fr/internet/communiques/telecharger.php?f=851ddf5058cf22df63d3344ad89919cf

motion picture studios to increase by 6.5-8.5%".[673] That said, it has to be noted after Watson et al that the data gathered by Danaher and Smith does not make it possible to determine whether the increase in movie sales following the shutdown lasted beyond the eighteen week follow-up period.[674]

While the studies cited above are only related to audiovisual works, not telling us much about the impact on the music/software/gaming industries, it is quite possible that the statistics they present are relatively accurate, and taking down Megaupload indeed caused an increase in the usage of legitimate services. However, a wider look at the Alexa web traffic rankings[675] puts this finding in a slightly different light. While some of the filesharing websites took the described actions following the incident, those that stayed fully operational experienced a considerable growth in popularity. In terms of the global traffic ranking, Rapidshare rose from 230th place on 18th January 2012 (the day before the takedown) to 160th place in the beginning of April 2012.[676] Mediafire rose from 75th position on 18th January to 67th in the beginning of April[677] – and if we consider that it means the 67th most popular website in the whole cyberspace, this rise is particularly significant. Uploaded.to, despite the US IP address block,[678] rose from 700th position on 18th January to 300th in the beginning of April.[679] Torrentz.eu, one of the largest BitTorrent meta-search engines, experienced a steady growth between 18th January and the beginning of April, from 150th to 120th position.[680]

---

[673] ^Supra fn. 646, at 1.
[674] Watson S, Zizzo D, Fleming P 'Determinants and Welfare Implications of Unlawful File Sharing: A Scoping Review' (2014) CREATe Working Paper 2014/05, available at http://www.create.ac.uk/wp-content/uploads/2014/04/Working-Paper-2014-15.pdf
[675] See http://www.alexa.com/ It has to be remembered that using such traffic data is subject to certain methodological limitations, and it should not be regarded as infallible. Firstly, there are dozens of factors which might cause a change in the amount of traffic a website receives. Just as with using GDP, one has to be careful not to attribute a noticed shift to a particular cause too hastily. Secondly, traffic data is prone to being compromised through, for example, the use automated bots artificially increasing a website's numbers.
[676] See http://www.alexa.com/siteinfo/rapidshare.com
[677] See http://www.alexa.com/siteinfo/mediafire.com
[678] See https://torrentfreak.com/uploaded-to-blocks-us-visitors-120121/
[679] See http://www.alexa.com/siteinfo/uploaded.to
[680] See http://www.alexa.com/siteinfo/torrentz.eu

There is little doubt that in order to fully assess the impact of such a takedown, further, more organised, web traffic-based research would be required – for example, it is quite difficult to tell how many users of Megaupload migrated to various P2P services. However, given the data presented in this section, it seems feasible to say that closing down Megaupload on the basis of criminal charges might have caused a moderate (though potentially temporary) rise in the popularity of legitimate services (most notably those focused on video streaming), along with a clear rise in the popularity of other websites used to obtain copyrighted material illegally. It is more than likely that a significant altsources migration took place after the shutdown.

Another example of an enforcement scheme which is likely to be encountering the challenge in question are the website blocking injunctions described above in section 3.1.2.3.1 of chapter two. Even if we assume that, for example, the Newzbin 2 injunctions are flawlessly removing access to the targeted websites (what is unlikely to be the case[681]), the game of cat and mouse continues due to the earlier mentioned abundance of alternative sources of infringing content.

A study conducted by Poort et al[682] might provide us with data confirming the impact of altsources migration on the blocking injunctions' effectiveness. The indicated researchers sought to assess the effectiveness of The Pirate Bay's ISP blockade in the Netherlands, prompted by the relevant court orders.[683] To this end, they relied on two sources of data – a customer survey and BitTorrent traffic observation. They found that the blockade had no lasting impact on the percentage of Dutch citizens downloading copyrighted material from illegitimate sources.[684] While BitTorrent participation decreased a little,[685]

[681] See section 2.3 of the current chapter.
[682] Poort J, Leenheer J, Van Der Ham J, Dumitru C 'Baywatch: two Approaches to Measure the Effects of Blocking Access to The Pirate Bay' (2013), available at http://ssrn.com/abstract=2314297
[683] Judgements of the Rechtbank's Gravenhage from the 11th of January and the 10th of May 2012.
[684] Poort et al, supra fn. 682, at 1.

Poort et al also discovered that the Dutch users searching for copyright-infringing material found alternatives to TPB, and switched over to them.[686] In conclusion – "the market has returned towards the earlier equilibrium, with only very small structural effects".[687] And while this study was focused on the ISP-level blockade, its findings could very well be applied to the enforcement approaches based on removing access to online intermediaries through domain name seizures and DNS blockades.[688]

The third and final enforcement scheme used in this section to demonstrate and discuss the altsources migration is the graduated response approach.[689] The empirical data gathered with regards to this scheme's effectiveness indicates that the altsources migration is one of the key challenges that this enforcement approach might face on the road to effective enforcement of copyright.

In 2009, the Digital Britain Report sought to support the enactment of the Digital Economy Act 2010 by stating that "there is evidence that most people who receive a notification stop unlawful file-sharing".[690] The said evidence was obtained from surveys, which "found significant numbers of people say they would stop or significantly reduce" their filesharing habits after the receipt of the said notification.[691] It is unclear whether the report referred to P2P filesharing, or to copyright-infringing filesharing across all possible online resources; the following paragraphs submit an argument that only the former version could be reflecting the actual behaviour of online infringers.

---

[685] Only small changes in the distribution of Dutch BitTorrent peers were found over the course of the three traffic measurements – Poort et al, supra fn. 682 at 11.
[686] Poort et al, supra fn. 682, at 2.
[687] Poort et al, supra fn. 682, at 12.
[688] See section 3.1.2.3.2 of chapter two for the discussion of the DNS blocking mechanisms.
[689] Covered in section 2.4 of chapter two.
[690] *Digital Britain: Final Report* (2009) by DCMS & BIS, at 111.
[691] *Digital Britain: Final Report*, supra fn. 690, at 111.

To this end, this section turns towards the empirical data gathered on the performance of the French take on the graduated response, the HADOPI law.[692] The first source of such data to be discussed is an official report released in 2009 by the agency operating the scheme.[693] The report offers three main findings in support of HADOPI's effectiveness. Firstly, it notes that between October 2010 and December 2011, 95 % of the (alleged) infringers who received the initial email, did not get the official letter.[694] Further 92 % of those who did receive the letter did not get to the third strike stage.[695] Those figures are interpreted as showing that a vast majority of users who were targeted by the "soft" measures of the HADOPI law, ceased their infringing actions. Secondly, the report states that 71 % of people who reached the "third strike" contacted the agency, which is regarded by the HADOPI agency as a factor "consolidating the change in behaviour"[696] (though it is not explained how). Finally, the discussed publication presents data from four external reports, showing a decline in P2P filesharing (both legal and copyright-infringing) in France in 2011. Depending on the external report, the general amount of filesharing is supposed to have decreased by 17% or 29%, and the amount of copyright-infringing filesharing is supposed to have decreased by 43 % or 66 %.[697]

However, as it was mentioned in the introduction to this chapter[698] the logic behind online copyright enforcement measures should likely be that a decrease in the amount of infringing activities should bring about an increase in the profits of copyright owners wishing to profit from the previously infringed goods. Unfortunately, the overall revenue of the French music industry decreased in 2011,[699] and so did the revenue of the French film industry.[700]

---

[692] HADOPI law, supra fn. 331.
[693] *Hadopi, 1,5 year after the launch* (2012) by the HADOPI agency, available at http://hadopi.fr/sites/default/files/page/pdf/note17.pdf
[694] *Hadopi, 1,5 year after the launch*, supra fn. 693, at 3.
[695] *Hadopi, 1,5 year after the launch*, supra fn. 693, at 3.
[696] *Hadopi, 1,5 year after the launch*, supra fn. 693, at 3.
[697] *Hadopi, 1,5 year after the launch*, supra fn. 693, at 3.
[698] See the beginning of section 1 of the current chapter.
[699] See http://www.telecompaper.com/news/french-online-music-worth-eur-110-mln-in-2011-study. The decrease occurred despite an increase in the revenue of legitimate online music services.

While there could of course be many factors behind this decline, the reported effectiveness of the HADOPI law could lead one to expect a clearly visible impact of the enforcement scheme on the profits of the said parties – and such an impact was not detected.

There are two main possible explanations of this status quo. Either the HADOPI agency's statistics were wrong after all, or (what is most likely the case) the majority of users who used to obtain their music and films from the targeted P2P networks migrated to other sources of copyrighted material, such as cyberlockers, streaming services, or P2P networks placed outside of the HADOPI's area of influence.

The report seeks to deny the existence of such a migration, showing that no significant increase in the activity of cyberlockers or "rogue" streaming websites was registered.[701] Unfortunately, this is where it commits a crucial and fatal methodological error, affecting its credibility with regards to the cited finding. The statistics used to back this statement up were based on the usage patterns of a representative panel of 25,000 French Internet users, who VOLUNTARILY installed metering software on their computers.[702] Would any dedicated illegal filesharer/downloader volunteer to have his movements tracked? The answer is practically certain; no. Not only due to the obvious risk of being caught: they would be participating in a research which ultimately might lead to the removal of their sources of free copyrighted material. Consequently, it is very likely that a significant altsources migration did occur as a result of HADOPI's activity – what would be also explaining why 95 % of those who received the first email did not get the second one. The UKIPO report support this critique of HADOPI's reasoning, stating that it "does not take into account whether the infringement has merely been displaced to

[700] See http://www.dvd-intelligence.com/display-article.php?article=1676
[701] *Hadopi, 1,5 year after the launch*, supra fn. 693, at 7.
[702] *Hadopi, 1,5 year after the launch*, supra fn. 693, at 7.

technological channels that are not being monitored for infringement".[703] While the HADOPI law might have indeed decreased the presence of certain forms of copyright-infringing P2P filesharing in France, it seems to have failed in significantly decreasing the amount of online piracy in general, which is ultimately the scheme's overarching goal.

In their article from 2013, Lauinger et al noted that the cyberlockers' "ecosystem has grown so diverse that there is no single indispensable actor"[704] – and it is hard to disagree, given that, for example, their study discovered copyright-infringing links leading to one-click-hosting websites on 9,825 different domains,[705] with many indexing websites oftentimes enclosing links to multiple cyberlockers per piece of infringing content. However, the conclusion about the ecosystem's diversity could very well be extended to the whole realm of copyright-infringing filesharing – in fact, there is no single, indispensable *platform* of infringement, given the variety described in chapter one above.[706] At the moment, as long as the demand for free copyrighted content lasts (and there is no reason why it should disappear), there will be new and old service providers, as well as uploaders of the content in question, ready to fill in the gaps in the ecosystem – despite the effects of the currently endorsed enforcement mechanisms.

As for the three categories of infringing content other than that which breaches copyright,[707] the enforcement schemes aimed at them might also be affected by the altsources migration; though the degree of its influence depends on which type of content the schemes are dealing with. If we look at trademarks and the *Akanoc* case described above,[708] a website hosting email addresses of Chinese companies making and distributing counterfeit products might be

[703] *International Comparison of Approaches to Online Copyright Infringement* (2015) UKIPO, at 5.
[704] Lauinger et al, supra fn. 651, at 9.
[705] Lauinger et al, supra fn. 651, at 10.
[706] See section 2.2 of chapter one.
[707] (Which are, it should be added, much more starved for empirical research demonstrating altsources migration than copyright is.)
[708] *Louis Vuitton v Akanoc*, supra fn. 168, case covered in section 3.2 of chapter one.

replaced by another one, hosting the same information. Counterfeit sellers challenged by the steps undertaken by certain auction/shopping sites might migrate to platforms with more lenient enforcement approaches – a shift noted by the EU Commission in 2013.[709] However, if we consider privacy-infringing and defamatory content, it is arguably much less likely to find online users seeking for sources of such content; it is probably more often the case that they are looking for various kinds of information about a specific party/parties, and defamatory or privacy-infringing content happens to be flowing between the pieces of legitimate content.[710] Furthermore, save for services such as, for example, revenge pornography websites,[711] or websites focused on leaked celebrity photos, it is very rare to hear about access to an online resource being removed due its role in the process of sharing privacy-infringing or defamatory content; hence, the altsources migration is relatively less of a challenge for the sector of enforcement policy aimed at those content types.

2.3. Circumvention of the technological aspects of the enforcement schemes.

It should be quite clear by this point of the thesis that many of the enforcement schemes described in chapter two are dependent on certain technological components. Blocking injunctions require adequate traffic blocking software, finding out an infringer's identity requires a procedure reliant on information such as the IP address; and a scheme such as DRM is entirely based on the technology aimed at limiting the user's interaction with the digital content subjected to such protection.

[709] Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet (2011), at 13, available at http://ec.europa.eu/internal_market/iprenforcement/docs/memorandum_04052011_en.pdf
[710] Though it could also be argued that frequent visitors of celebrity-gossip websites love to see nothing more than content such as news or images exposing celebrities' private lives.
[711] Described in section 4.2 of chapter one.

However, many of those technological components are susceptible to various forms of circumvention; and such a weakness is oftentimes exploited by those wishing to share or facilitate the sharing of infringing content – primary that which infringes copyright. As O'Sullivan writes, "the reality remains that (1) circumvention measures are easily accessible; (2) limited technical skill is required for use; and (3) use demonstrates that internet users are not discouraged by complicating factors".[712] This section of the chapter seeks to demonstrate how such circumvention might come to pass. In contrast to sections 2.1 and 2.2, the following paragraphs contain more distinct examples of the challenged enforcement schemes, due to the fact the each method of circumvention is different, depending on the technology being circumvented.

The first group of enforcement schemes to receive attention in this section are, once again, those which seek to remove access to online resources used for infringing purposes, with the increasingly popular ISP-oriented blocking injunctions starting us off. While the shutdown of Megaupload is probably the most eminent example of the criminal law approach based on website takedowns, it is difficult to find a "pirate" website which would be the subject of more ISP-blocking attempts than TPB. However, the available evidence seems to suggest that such blockades are far from being impenetrable. For example, if we look at the Dutch attempt on this field, an empirical study conducted by van der Ham et al[713] (focused on the observation of BitTorrent traffic through a sample of copyright-infringing torrents) has shown that the blockade of TPB had "no significant measurable effect"[714] on the BitTorrent traffic in Netherlands. Such a result might not come as much of a surprise, given that - according to Lodder and Meulen – TPB has over a hundred IP addresses at their disposal[715] and the website's operators might jump from one address to another, circumventing the blockade. This is oftentimes enabled by

[712] O'Sullivan K, 'Enforcing copyright online: internet service provider obligations and the European Charter of Human Rights' (2014) 36(9), at 581.
[713] Van der Ham J, Rood H, Dumitru C, Koning R, Sijm N, De Laat C, *Review en Herhaling BREIN Steekproeven* (2012), available at https://staff.fnwi.uva.nl/j.j.vanderham/research/publications/dutchpirate.pdf
[714] Van der Ham et al, supra fn. 713, at 18.
[715] Lodder and Meulen, supra fn. 643, at 135.

the website operators shifting their hosting providers to ones located in countries which are more lenient/less active in the area of online enforcement – for example, TPB was hosted in Ukraine,[716] and a major Polish cyberlocker, chomikuj.pl, changed their hosting to Cyprus.[717]

However, is the intermediaries' IP-hopping practice (mentioned earlier in this section) the only method of circumvention standing behind such poor results? In order to find an answer to this question, it is worth taking a closer look at Cleanfeed, the filtering system employed by BT: initially, to combat child pornography in cooperation with the Internet Watch Foundation,[718] later on - in order to implement the *Newzbin2* court orders. It is a hybrid blocking system, composed of router-based IP blocking and a form of deep packet inspection focused on blocking URLs. In this section, it is sufficient to focus on the former, while the latter receives further coverage in section 2.3.1.2 of chapter five. In the described context, Cleanfeed works in the following manner: firstly, an ISP subscriber enters a domain name into his Internet browser. The browser then retrieves the IP address associated with that domain name from a Domain Name Server (most often the ISP's); if the retrieved IP address is on the Cleanfeed system's blacklist, the so-called border gateway routers responding to the demands either block the connection, in which case the user receives a 404 error (page not found), or redirect him to another page instead of being transferred to the blocked webpage.

An advantage of using this system is that it cannot be circumvented simply by typing in the website's IP address, unlike certain forms of DNS blocking (see below). That said, as Clayton rightly noted in his article, the system is vulnerable to other forms of user circumvention.[719] First and foremost, users might disguise the final destination of the requested traffic through the use of

[716] See https://torrentfreak.com/chased-from-sweden-pirate-bay-sails-to-ukraine-091002/
[717] See http://prawo.gazetaprawna.pl/artykuly/456064,chomikuj-pl-uciekl-wydawcom-na-cypr.html (in Polish)
[718] Uniform Resource Locators – ie. a web address.
[719] Clayton R, 'Failures in a Hybrid Content Blocking System' (2005), available at http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf

proxy servers/Virtual Private Networks (hereafter referred to as VPNs), transforming the client's IP address into one provided by the ISSP; and the use of networks such as TOR or JAP, which hide the traffic and IP address under a layer of multiple transfers taking place between the users' PCs.[720] Additionally, a suggestion has been made on the Open Rights Group wiki, that Cleanfeed only blocks traffic from the TCP port 80 (responsible for "normal" websites' http traffic), which means that accessing the blacklisted website through, for example, the https protocol,[721] might not be affected by the filtering procedure[722] - though the described method does not seem to be working in 2016. Concluding, it seems that in the view of both intermediaries' and infringers' circumventing efforts and possibilities, the long-term effectiveness of Newzbin 2 injunctions can be questioned – despite the signs of effectiveness referred to in the *EMI* case, such as the Alexa rankings showing that within a year from the *Dramatico (No.2)* case, TPB felt from 43rd to 293rd place in UK, and the Italian TPB blocking order causing a 73 % reduction of access in Italy and a 96 % reduction in page views.[723] This is even more likely to be the case given the fact that both of those pieces of evidence might be distorted by the use of VPNs.

Let us now consider another major method of filtering out the websites used for infringing purposes, a system which was supported in the draft of the US Protect IP Bill:[724] the DNS filtering. At first glance, its core idea seems promising; if an Internet user typing in the domain name of a blocked website is not going to be connected to it, the infringing activity is not going to take place. Additionally, as Ou points out, DNS filtering proved to be a fairly efficient technology in combating the spread of malicious software attacks, such as those conducted by botnets.[725]

---

[720] Clayton, supra fn. 719, at 7. That being said, it has to be mentioned that the findings of a paper from 2005 are at risk of being out of date – it would be beneficial to have similar research conducted in the coming years.
[721] See http://en.wikipedia.org/wiki/HTTP_Secure
[722] See https://wiki.openrightsgroup.org/wiki/Cleanfeed
[723] Italian TPB blocking order, supra fn. 119, at [106].
[724] Protect IP bill, supra fn. 551.
[725] See http://www.hightechforum.org/dns-filtering-is-essential-to-the-internet/

Unfortunately, the DNS filtering technology can be circumvented in several ways; and none of them requires the Internet users to become grand masters of network hacking. First of all, the blocked website might be rehosted under a different domain name, what makes it available again. The challenge here for the website's operators is to spread the new domain name among the Internet users wishing to find the rehosted website. However, keeping in mind the eagerness of the online community to share such data,[726] it should not be too difficult. Indeed, this method of circumvention proved to be successful when Rojadirecta (a sports streaming website) had its domain name (rojadirecta.com) seized[727] – it was rehosted under the name rojadirecta.es, and as Alexa ratings show,[728] it quickly became as popular as the original domain. While Rojadirecta transferred to a Spanish ".es" domain, it seems fitting to remark here upon a certain trend present among the operators of filesharing-oriented websites, to endorse domain names registered in places such Tokelau Islands (.to – for example, uploaded.to) or Cocos Islands (.cc – for example, extratorrent.cc). It is more difficult for the copyright enforcers to block (or seize) such domains. Additionally, it is worth noting on this occasion a point made by Lauinger et al about a peculiar characteristic of indexing websites (such as those used for indexing the content of cyberlockers): they are much more flexible when it comes to being rehosted under a different domain name (or IP address), due to the lower bandwidth requirements[729] (a link to a file hosted on a one-click-hosting website "weighs" significantly less that the file itself). Both observations made in this paragraph enhance the notion of DNS-oriented measures' vulnerability.

The second method of bypassing a DNS filter is extraordinarily simple - though it applies only to the simplest forms of such blocking mechanisms. As explained in section 3.1.2.3.2 of chapter two, the DNS filtering injunctions are

[726] See section 5 of the current chapter.
[727] See https://torrentfreak.com/us-resume-file-sharing-domain-seizures-110201/
[728] See http://www.alexa.com/siteinfo/rojadirecta.com and http://www.alexa.com/siteinfo/rojadirecta.es
[729] Lauinger et al, supra fn. 651, at 13.

focused on severing the connection between the targeted website's domain name and its respectable IP address.[730] However, should the user type in the website's IP address directly (with the filtering system containing no additional protections), he would be bypassing the DNS filter completely. And once again, due to the peculiar character of modern day's online community, the IP addresses of websites used for, for example, online copyright infringement are likely to be swiftly spread around the cyberspace, if the situation calls for it. It is worth adding that this method of circumvention might also affect the domain name seizures, endorsed by, for example, the PIPCU.[731]

Thirdly, the online users can obtain specific software, such as the MAFIAAFire Redirector add-on for web browsers, which is specifically designed to bypass the DNS filters. The significance of this method of circumvention is, to a certain extent, enhanced by the fact that Mozilla refused to obey the request to remove this software from its official add-on website;[732] and at the time of writing continues to do so.[733]

Finally, the Internet user can change their DNS service provider for one which is outside of the scope of the user's country's jurisdiction, and does not implement DNS filters covering the targeted website. And, as the White Paper published by a group of DNS experts in response to the Protect IP Bill stated, pirate websites are more than happy to assist their users in performing such a switchover (which can be performed by changing one line of code on the user's computer).[734] That said, even if a user knows how to do it, he might not be keen on making his personal data visible to the operators of a potentially

[730] See section 3.1.2.3.2 of chapter two.

[731] See http://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/pipcu-news/Pages/PIPCU-assists-in-suspending-188-websites-.aspx

[732] See http://arstechnica.com/tech-policy/2011/05/mozilla-resists-us-govt-request-to-nuke-mafiaafire-add-on/

[733] See https://addons.mozilla.org/en-US/firefox/addon/mafiaafire-redirector/

[734] Crocker S, Dagon D, Kaminsky D, McPherson D and Vixie P 'Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill' (2011), available at http://www.circleid.com/pdf/PROTECT-IP-Technical-Whitepaper-Final.pdf, at 8.

"rogue" DNS service. While the earlier mentioned experts' report states that "the user who is seeking pirated content ... will often be more concerned about getting the content than with how reputable a particular DNS provider might be",[735] it is more than likely that the majority of modern day downloaders would not put their privacy and security at stake to obtain a few copyrighted files, especially given the amount of alternative sources of such material. Then again, it is not always the "rogue" DNS providers which are used for this method of circumvention – for example, when circumventing the Twitter blockade in Turkey, the users relied on the Google DNS service.[736]

Two additional observations might be made with regards to the circumvention of website-blocking measures such as IP and DNS filtering. The first one relates to the BitTorrent networks; as it might be remembered, section 2.2.3.1 of the first chapter described the mechanics of BitTorrent filesharing and the role played by torrent trackers. As it might also be remembered, websites such as The Pirate Bay, Oink's Pink Palace or Filesoup became targeted by the enforcement bodies precisely because they ran torrent trackers facilitating the spread of infringing content in cyberspace.[737] However, as Manner et al rightly note, there is a tendency amongst many filesharers to forego reliance on the torrent trackers for the sake of the Distributed Hash Table (DHT) torrenting,[738] which is more focused on the connections between the users' computers and does not require a centralised torrent tracker. The movements towards solutions like DHT could be seen as a way of circumventing the enforcement schemes aimed at websites running torrent trackers, because the latter cease to be an essential component of BitTorrent filesharing.

The second observation follows, in a way, the remark made above about the intermediaries being able to rehost their websites under a different domain

[735] Crocker et al, supra fn. 734, at 8.
[736] See http://torrentfreak.com/turkeys-twitter-ban-collapse-fueled-by-vpns-and-dns-tricks-140322
[737] See section 2.2.3.1 of chapter one.
[738] Manner M and others, 'The Pirate Bay ruling – when the fun and games end.' (2009) Ent.L.R. 20(6), 197, at 198.

name in order to bypass the DNS-oriented measures. It has to be reiterated that website operators might also challenge the enforcement schemes aimed at removing access to the "infringing" websites by changing the latter's hosting providers. As Lodder and Meulen notice, TPB is a particularly good example here, having been hosted in countries such as Sweden, Germany, or Ukraine.[739] Such an approach makes it considerably more difficult for the enforcers to remove access to a website by contacting its hosting providers. Furthermore, to quote Lauinger et al – "(i)t is not unusual at least for larger indexing sites to have servers located in different countries, with the true locations often being hidden behind a load balancing or anti-DDoS service".[740]

Moving away from the access removal measures, let us look at the other enforcement schemes vulnerable to circumvention – notice and takedown and preventive filtering being the first such examples. Section 2.1 of this chapter described how infringing content often comes back to the same platform with the help of practices such as changing the file's name or modifying the elements of the file used by the filtering systems. It is worth remarking upon another form of circumvention used within the indexing websites, that is the practice of using masking services such as Linksafe,[741] which might aid in protecting the links to infringing content from being automatically removed by the content filtering systems.[742] Furthermore, a recent milestone empirical study (conducted by Urban et al) indicated in 2016 that filesharing websites tend to rely on automated means of protecting their files from notice and takedown, such as automated multi-upload software.[743]

Identification measures, covered in chapter two,[744] are also challenged by various forms of circumvention, which are by far not limited to using an alias. As Friedmann noted, online infringers have a tendency to cover their tracks,

[739] Lodder and Meulen, supra fn. 643, at 138.
[740] Lauinger et al, supra fn. 651, at 10.
[741] See http://linksafe.me
[742] Lauinger et al, supra fn. 651, at 3.
[743] Urban et al, supra fn. 458, at 33
[744] See section 2.3 of chapter two.

which often makes it difficult to implement the enforcement schemes built around, for example, civil damages or the graduated response.[745] It is plausible to agree with Farrand, who wrote in 2010 that dedicated infringers are likely to use VPNs and hide their IP addresses.[746] Given the likely spread of such methods to the less experienced infringers, it is a concern to be reckoned with.

Finally, there are various forms of DRM, which have been widely circumvented for decades now – even before the cyberspace era. The author recalls seeing multiple stands in his city market, offering a range of cracked CDs and DVDs, with fake labels affixed to their covers with paper glue. In the era of online piracy, the widespread use of DRM-breaking software is one of the key reasons explaining how various filesharing platforms became filled to the brim with copyright-infringing content. A significant role in this process was, and continues to be, played by the release/warez group, such as the one mentioned above in relation to the case of *Griffiths*.[747] Additionally, to provide a more recent example; in late 2015, the AudioUTOPIA group cracked the iLok2 system, protecting high-end audio software, what prompted the proliferation of the latter in the filesharing ecosystem.[748] The most established groups of this kind have released thousands of movies, music tracks, PC games etc. into the cyberspace, oftentimes very shortly after the release of the legitimate original. While certain forms of DRM could be seen as quite effective, for example those encountered in the PC games sector (for example, the Steam platform,[749] the Diablo 3's "always online" requirement[750]), it is extremely difficult to say that the DRMs have been even mildly effective in the online struggle against copyright-infringing content in general.

[745] Friedmann D, 'Sinking the safe harbour with the legal certainty of strict liability in sight' (2014) Journal of Intellectual Property Law & Practice 9(2), at 149.
[746] Farrand B, 'The Digital Economy Act : cause for celebration or cause for concern?' (2010) E.I.P.R. 32(10), 536, at 539.
[747] *Griffiths v USA*, supra fn. 354.
[748] See https://torrentfreak.com/ilok2-drm-system-appears-to-have-been-cracked-151224/
[749] See http://store.steampowered.com/about/
[750] Described in section 2.5 of chapter two.

In the earlier mentioned study conducted by Poort et al, the authors submitted, after the analysis of the BitTorrent traffic data, that a certain degree of the "learning effect" could be observed among the users who were meant to be prevented from illegal filesharing by the ISP blockade of The Pirate Bay.[751] It is most likely that many of those users learned how to circumvent this blockade. Having shown a wide variety of ways in which the enforcement schemes are circumvented by both infringers and intermediaries, this section submits that such a "learning effect" has developed not just in the field of ISP blockades, but in the whole ecosystem of copyright-infringing filesharing – and this development is likely to continue, with the new methods of circumvention likely to appear on the scene in the coming years, and potentially, crossing over to other content type areas.

3. Deterrence effect of the enforcement schemes.

When looking at the challenges identified in the first subchapter, one might wonder whether there are any factors connecting them, whether there are any weaknesses of this branch of online enforcement which could be seen as standing behind the three described primary problem areas; it is submitted that the lack of deterrence is a major weakness of this kind. Consequently, the purpose of the current subchapter is twofold - firstly, it seeks to demonstrate how various enforcement schemes are lacking the deterrence effect; and secondly, to explore why it is so. Due to the difference in the perspectives of the infringers and the intermediaries, a further division is made, on two further sections; with 3.1 focused on the deterrence of infringers, and 3.2. focused on the deterrence of the intermediaries.

3.1. Deterring infringers.

[751] Poort et al, supra fn. 682, at 11.

The second subchapter provides us with multiple examples of enforcement schemes failing to deter the infringers from obtaining or spreading the infringing content in cyberspace. Notice and takedown and preventive filtering are definitely amongst them – as section 2.1 shows, numerous copyright-infringing users whose content was taken down are unlikely to be deterred from reuploading it, and neither are the downloading users likely to be deterred from their activity by the fact that the content they sought to obtain was identified as illegal and taken down. In the realm of trademarks, counterfeit sellers on eBay are also unlikely to be discouraged from their endeavours upon seeing their sale offers taken down. As for privacy and defamation, there might be a higher presence of the deterrence factor; that is unless the infringer is unusually dedicated, for example, to spreading personal or defamatory material concerning the rightholder.

The preceding paragraphs of this chapter also contain evidence indicating that the threat of civil and criminal liability does not seem to always act as a strong enough deterrent, capable of preventing multiple infringers from, for example, reuploading the infringing content, moving to alternative sources of such content or circumventing the technological aspects of the enforcement schemes. This would be in accordance with Eziefula's article from 2011, where he wrote that in the copyright context, the early attempts to sue small scale infringers can be seen as a signal failure.[752] Regarding the graduated response, the discussion of its effectiveness set out above[753] seems to indicate that, while this enforcement scheme might deter some users from using the BitTorrent network, it is unlikely to discourage them from looking for alternative sources of copyright-infringing content.

One could also expect that the removal of access to an infringing platform, especially when conducted in the form of a criminal law-based shutdown (for

[752] Eziefula N, 'Getting in on the Act - OfCom publishes draft code on Digital Economy Act initial obligations' (2010) Ent. L.R. 21(7), 253, at 253.
[753] See section 3.1.1.2 of the current chapter.

example, Megaupload, TV Links[754]), would act as a deterrent for the infringing users of the said platform. Firstly, it makes it clear that the users' actions were linked to an illegal activity, one carrying the criminal stigma. Secondly, the users could be deterred by the possibility that their files and/or personal data might enter the hands of the enforcement bodies, which might then turn the obtained material against them. However, the evidence discussed in the previous sections of the chapter indicates that such a deterrence effect is currently rather limited. Such a position is likely to be even truer in the case of blocking injunctions, where the described criminal stigma and risk of repercussions is considerably lower.

Lastly, it is quite clear at this point that the deterrence effect of various forms of DRM is nearly non-existent, despite the legal protection given to this enforcement scheme by the Infosoc Directive.[755]

Now, it has to be remembered that pointing out the enforcement schemes' shortcomings in the field of deterrence should not be conducted without mentioning the but-for test; ie. what would happen to the current level of infringing activity in cyberspace if the said enforcement mechanisms were not endorsed at all within the European Union? Specifically for this section, would online users be more inclined to obtain and/or spread the infringing content than they are now? Due to the (rather understandable) lack of suitable data, we can only imagine that without the currently endorsed enforcement schemes, the cyberspace would be a true bonanza of digital content infringing the four legitimate interests this thesis is focused upon. Legitimate sources (both online and offline) of digital copyrighted content would go out of business, auction websites would be filled with trademark-infringing counterfeit offers, people's private information would be constantly flying around the Net without stopping for the red light, and blatantly defamatory material would be found at every second turn of the Internet's pathways. It has to be remembered that the

[754] See section 3.2 of chapter two.
[755] See section 2.5 of chapter two.

presently employed enforcement schemes DO carry a measure of the deterrence effect, which prevents the current and potential infringers from going on a rampage. However – this does not mean that the shortcomings identified in the beginning of this section are less concerning, or that we should not explore the possibilities for improvement in this regard.

One of the preliminary steps which might lead us to such an improvement is understanding the decision-making process of the online infringers, preceding their illicit activities. While the factors affecting it are likely to be different depending on the type of infringing content at hand, the scoping review conducted by Watson et al (in the field of copyright) might provide us with a starting point of analysis. The researchers in question identified five primary categories of factors affecting a person's decision on whether to obtain copyright-infringing material through illegal filesharing.[756] The first of such categories is characterised as the legal and financial net utility, and covers factors such as the risk of being subjected to legal and financial repercussions following detection. The second one was given the name of experiential net utility, and embodies the individual's desire to experience the copyrighted material at hand. Next is the technical net utility, representing the individual's perceived or actual ability to obtain the said material, for example, how well versed they are in BitTorrent filesharing, or what kind of hardware do they have at their disposal. The fourth category to be identified is social net utility, which focuses on the influence which the society might exert on an individual engaged in copyright-infringing filesharing, for example, whether his/her peers support online piracy or not.[757] The last one of the five is stated to be the moral net utility, which covers the person's individual beliefs on what is right or wrong.

[756] Watson et al, supra fn. 674, at 27.
[757] For further discussion of the social deterrence effect, see section 5 of the current chapter.

It has to be noted at this point (just as the authors of the report did[758]), that the categories listed above relate only to the factors affecting the decision-making process of the *downloading* infringers, ones obtaining the content; the said categories are not drafted with the uploading/contributing infringers in mind. While the latter category is also likely to be considering the legal and financial, technical, social and moral net utilities of their actions,[759] the experiential net utility (as it is described) does not seem to suit the individuals who already have access to copyrighted content, but want to share it with others nevertheless. In order to fit such users' decision-making process, experiential net utility could be refocused so as to cover factors such as the desire to share information with other Internet users, in order to connect them to one's own experience derived from the copyrighted content at hand.

Having drawn that distinction, we can ask the following question: which of the five categories of the decision-influencing factors can be affected by the legal enforcement schemes such as those described in chapter two? The experiential net utility seems to be outside of their reach; they cannot really decrease the people's desire to experience or share various forms of infringing content. As for the technical net utility, restricting the spread of knowledge on how to use various methods of sharing information online does not seem to be the most feasible option; trying to, for example, pursue websites or individuals who share such knowledge is likely to cause a backlash effect. That being said, successful removal of access to platforms used for infringing purposes could be one of the directions to follow in order to deter infringers; an individual's drive to obtain copyright-infringing content might be tampered when placed against the exhaustive feeling coming from being unable to discover the new online resources containing the desired material. So far, it is fairly clear that the presence of alternative resources of this kind remains high, despite the multiple legal efforts described in chapter two. Nevertheless, a certain side note could be made here with regards to the copyrighted content; it should be noted that since consumers generally wish to obtain digital copyrighted goods

[758] Watson et al, supra fn. 674, at 11.
[759] (Though in a different manner.)

in the most comfortable manner available, the distributors of the legitimate copyrighted content should strive to make their services *at least* as comfortable in use as the pirate resources are.[760] Such a notion is supported by Watson et al, who found out that for many consumers the illegitimate sources of copyrighted content were more efficient and flexible than the legitimate ones.[761]

Social net utility is also likely to be outside of the enforcement schemes' direct reach, together with moral net utility.[762] Therefore, out of the five categories of factors which affect the individual's decision to infringe, it is the legal and financial utility (with the risk of punishment being the key factor) which can be affected the most by the measures described in chapter two. A study conducted by Adermon and Liang,[763] which analysed the aftermath of the Enforcement Directive's implementation in Sweden, seems to be supporting this position. It was thought that transferring the art. 15(2) of the said Directive[764] (enabling the identification of potential infringers) into Swedish law is going to act as a deterrent against the copyright-infringing filesharers. And indeed, the cited researchers found that the law reform decreased the Internet traffic in Sweden by 16 percent during the first six months. Assuming that roughly half of the Internet traffic is thought to consist of online piracy,[765] the researchers stated that we could be considering here a decrease of copyright-infringing filesharing by 32 %. [766] However, it was also found that the Internet traffic "almost completely recovered after six months"[767] – according to researchers, this occurred due to the fact that only a few legal

[760] This means giving attention to factors such as content availability, quality of the transfer connection or indexing quality.
[761] Watson et al, supra fn. 674, at 39.
[762] They could potentially be affected through the influence exerted upon the legal and financial net utilities; for example, people might not wish to be too close to a person convicted of criminal copyright infringement.
[763] Adermon A and Liang C-Y 'Piracy and Music Sales: The Effects of an Anti-Piracy Law" (2014) Journal of Economic Behavior & Organization (105), 90.
[764] Described in section 2.3 of chapter two.
[765] This is supposedly according to Schultze H and Mochalski K, 'Internet Study 2008/2009'(2009), available at http://www.ipoque.com/sites/default/files/mediafiles/documents/internet-study-2008-2009.pdf However, the cited White Paper does not seem to contain such a reference.
[766] Adermon and Liang, supra fn. 763, at 2.
[767] Adermon and Liang, supra fn. 763, at 2.

cases followed the law reform, with each of them staying in the court for a long time (the first one was decided 4 years later).[768] When it turned out that the actual risk of punishment for breaking the copyright law is much smaller than it was feared to be, the deterrence effect dissolved nearly as quickly as it appeared. A similar finding was reached in a study conducted by Hsu and Shiue in 2008.[769]

Another study which seems to be reflecting the strong influence of the risk of punishment on the decision-making process of a potential copyright-infringing downloader is one which was conducted by Lysonski and Druvusula in 2008.[770] The study was conducted by means of a survey, which was administered to a group of 364 students. The respondents were presented with four scenarios related to stealing music,[771] and were asked whether they would commit the act described in each of them, and whether they think their friends would do likewise. The first two scenarios were based on the act of stealing a physical CD from a music store - the first one with a 100 percent certainty of not getting caught, the second one with some chance of being caught by an invisible security camera. The remaining two scenarios described the acts of downloading music illegally from the Internet.

The results obtained by the researchers have shown that while the respondents were overall very unlikely to steal the physical CDs from the music store, around a half of them indicated that they would commit the acts of downloading described by the third and fourth scenario.[772] Lysonski and Druvusula concluded that this indicates the existence of a strong correlation between the threat of punishment and the Internet user's decision to download copyrighted files illegally.[773] Additionally, the results indicated that the

[768] Adermon and Liang, supra fn. 763, at 3.
[769] Hsu J, Shiue C 'Consumers' willingness to pay for non-pirated software (2008) Journal of Business Ethics, 81(4), at 730.
[770] Lysonski S and Durvasula S 'Digital piracy of MP3s: consumer and ethical predispositions' (2008) Journal of Consumer Marketing 25(3), 167.
[771] Lysonski and Durvasula, supra fn. 770, at 171.
[772] Lysonski and Durvasula, supra fn. 770, at 173.
[773] Lysonski and Durvasula, supra fn. 770, at 175.

respondents regarded their peers as much more likely to commit each of the acts described by the representative scenarios - which reinforces the notion of social acceptance of infringing content, discussed below, in section 5 of the current chapter.

Concluding this section – assuming the purely effectiveness-oriented mindset for the moment, it seems that there are two primary paths which the enforcement bodies could take in order to successfully deter the online users from obtaining and/or sharing infringing content, and prevent new generations from growing up in the belief that there is no sanction for such activity (a risk noted by Cusack[774]). The first one is to make it so difficult and bothersome to commit those actions that people give up on them (ie. influencing technical net utility), the second one is to make the punishment so harsh and/or probable that people will not dare to break the law.

3.2. Deterring intermediaries.

Focusing on the enforcement schemes aimed at the intermediaries received a certain amount of support among the academic community. Davies wrote in 2011 that the "(p)rincipal reason for prosecuting website owners rather than end-users is that it is a more efficient and effective way of protecting copyright",[775] and Ginsburg submitted in 2008 that "meaningful copyright enforcement will seek to establish the liability of entrepreneurs".[776] Let us engage with those statements and commence this section by exploring whether such intermediary-oriented enforcement schemes brought about the deterrence effect to the ecosystem of online services facilitating the spread of infringing content in cyberspace.

[774] Cusack N, 'Is the Digital Economy Act 2010 the most effective and proportionate way to reduce online piracy?' (2011) E.I.P.R. 33(9), 559, at 559.
[775] Davies, supra fn. 357, at 395.
[776] Ginsburg, supra fn. 473, at 228.

Firstly, a certain crucial question has to be answered – what is it that we are trying to deter the intermediaries from? After all, not from committing the original acts of exchanging infringing content in cyberspace. It is submitted in this section that deterrence of intermediaries denotes discouraging them from either operating a service which facilitates the exchange of infringing information – or from operating it without taking sufficient precautions against the infringing use of their service.

Therefore, are intermediaries actually deterred by the currently endorsed enforcement schemes from pursuing the described activities? Some writers would seem to support an affirmative answer to this question. Davies indicated The Pirate Bay's case as an example of effectiveness, claiming that it has the potential to act as a strong deterrent against copyright infringement,[777] Tumbridge wrote about the *Fox v Newzbin*[778] case that it will doubtlessly lead to more cautious online behaviour,[779] and Lauinger et al considered that shutting down a website as large as Megaupload "may cause an increased perceived risk in the ecosystem".[780]

Indeed, some measure of the discussed deterrence effect could be observed in the recent years of this online enforcement struggle. If we take the criminal law-based shutdowns of websites facilitating copyright-infringing filesharing, the shutdown of Megaupload had (as it was mentioned in section 2.2 of the current chapter) at least some impact on the operators of other filesharing services. To recapture: in the days following the arrests, Filesonic and Fileserve have gone into a "no-sharing" mode, Uploaded.to banned connection requests from all US-based IP addresses, and at least two video streaming services (VideoBB and VideoZer) closed their affiliate programmes. Though, as noted by Danaher and Smith, Megaupload was an extremely popular

[777] Davies, supra fn. 357, at 390.
[778] *Fox v Newzbin*, supra fn. 122.
[779] Tumbridge J, 'A cunning Fox defeats the pirates: 20th Century Fox v Newzbin' (2011) E.I.P.R. 33(6), 401, at 404.
[780] Lauinger et al, supra fn. 651, at 11.

service: shutdowns of less prominent filesharing websites might be unlikely to have a similarly visible impact.[781]

Furthermore, there is evidence of the so-called "voluntary" shutdowns. These occur whenever an operator of a service facilitating infringements is deterred from running it, as a result of various forms of pressure. For example, NZBMatrix (Usenet website mentioned in chapter one[782]) shut itself down citing an overloading amount of received takedown requests (especially from major Hollywood movie studios) as the reason.[783] Another trigger of such shutdowns could be the "mere-prosecution" factor. In three out of the four UK cases presented in section 3.2.1 of chapter two (concerning TV Links,[784] Oink's Pink Palace,[785] and Filesoup[786]) the defendants were acquitted or their case was dropped by the CPS – however, none of the three websites returned to the cyberspace following the trials. There are two main lines of explanation here, which might have occurred simultaneously – firstly, the experience of going through a criminal trial might have discouraged the operators from maintaining/reviving those services (as in the TV Links case). Secondly, the disbandment of those websites' contributing users' communities (which is likely to follow such takedowns) might have made the return of the service pointless – after all, websites such as those are only platforms, they most often need active, contributing users to function. In any case, it seems that the mere fact of bringing in a prosecution might be achieving a measure of deterrence in itself. Additionally, sometimes even a threat of liability in itself might be enough to discourage an operator; like it happened with NZBsRus (another Usenet-oriented website which facilitated copyright infringement).[787]

[781] Danaher and Smith, supra fn. 646, at 24.
[782] See section 2.2.3.2 of chapter one.
[783] Supra fn. 102.
[784] *R v Rock and Overton*, supra fn. 90.
[785] *R v Allan Ellis*, supra fn. 113.
[786] The Filesoup proceedings, supra fn. 583.
[787] See https://torrentfreak.com/hollywoods-fact-forces-shutdown-of-nzbsrus-130627/

Finally, the fact that a considerable number of websites used for the exchange of infringing information operates notice and takedown schemes (oftentimes fairly efficiently) - with an occasional preventive filtering scheme being in place as well (for example, Content ID[788]) – can be seen as a testimony to the presence of the deterrence effect.

While the earlier mentioned but-for test has to be kept in mind,[789] the shortcomings in the effective deterrence of the intermediaries are also quite clearly visible. As Lauinger et al noted, after the shutdown of Megaupload, "even more new one-click hosting websites entered the ecosystem, despite the now apparent risks"[790] – which re-emphasizes the constant availability of online locations for the altsources migration. For a further example, the major streaming websites, such as Putlocker[791] or GorillaVid[792] continue to operate in cyberspace, together with the major stream-indexing websites (such as 1Channel[793]). Furthermore, it is difficult not to mention The Pirate Bay, which continues to thrive despite a guilty conviction for contributory copyright infringement secured against its operators in 2009,[794] multiple blocking injunctions and all the other legal efforts. And for a final, more recent example, the kino.to website (a streaming portal taken down by the police from several EU countries in 2011) came back online as kinox.to; and it is still available in the beginning of 2016.[795] It is difficult to perceive those instances as showing a "strong deterrent against infringing copyright".[796] Finally, the earlier mentioned affiliate programmes continue to be endorsed by many cyberlockers.[797]

[788] See section 3.1.2.2 of chapter two.
[789] See section 3.1 of chapter three.
[790] Lauinger et al, supra fn. 651, at 9.
[791] Now renamed to Firedrive, see http://www.firedrive.com/.
[792] See http://www.gorillavid.in
[793] Now renamed to Primewire, see http://www.primewire.ag/.
[794] TPB trial, supra fn. 111.
[795] See https://torrentfreak.com/kino-to-raided-in-massive-police-operation-admins-arrested-110608/
[796] Davies, supra fn. 357, at 390.
[797] For example, see http://rapidgator.net/article/resource

Therefore, a similar challenge arises here as it did in the previous section – *why* are multiple intermediaries not deterred from running their services in the manner which facilitates the exchange of infringing information? Again, the starting point for answering this question might be lying in understanding the factors which affect the decision-making process of such intermediaries, when they reflect on whether they want to continue operating their services.

In his article from 2002, Hardy attempted to identify the three main motivations driving the copyright infringers, motivations which might actually help in shedding light on the intermediaries'[798] perspective. These were: seeking commercial gain from dealing with infringing works, wishing to promote learning or creativity, and acting without a particular motive.[799] While this author believes that the third motivation would be better identified as, for example, a conscious or subconscious desire to enjoy the experience of sharing (or facilitating the sharing of) information with others, for the purpose of this thesis and this section, Hardy's division can be distilled into two motivations, dividing the relevant intermediaries on two groups – those who seek commercial gain, and those whose actions are driven by any other ideas, principles or desires.[800] Additionally, it is worth adding that the factors belonging to the earlier mentioned[801] legal and financial net utility (for example, the actual financial gain resulting from the legitimate and/or illegitimate use of the service, or the risk of punishment) are also likely to be applicable to intermediaries.

The relevant operators who seek commercial profit derive it from advertising and/or premium membership schemes. The most likely explanation for their resistance to the deterrence effect is that the profits they receive (or hope to receive) from maintaining their services overcome the perceived chance of

[798] Potentially not only the ones tied to copyright-infringing activities, but to other three content areas as well.
[799] Hardy I, 'Criminal Copyright Infringement' (2002) Wm. & Mary Bill Rts. J. 305, at 326.
[800] Though these motivations are not mutually exclusive, of course.
[801] See section 3.1 of the current chapter.

being targeted by the enforcement schemes described in chapter two.[802] This might be caused by, for example, the comparatively small amount of prosecutions conducted against the given category of online services or because their operators locate such services in countries which are not particularly active in enforcing the interests of the rightholders.[803]

In order to understand the most likely primary ideology driving the more idealistic operators, it is worth looking towards Schultz's article from 2007, where he refers to three principles originating from the "hacker culture", which might be influencing a fair amount of individuals operating websites used for infringing purposes (copyright-infringing ones in particular). These are: the belief that access to technology should be free, the belief that access to all information should be free, and a mistrust of the authorities.[804] This set of ideas seems to be fitting with the operators of websites such as The Pirate Bay, who are now regarded by some as the "online Robin Hoods", with their website being the digital flagship of online piracy.

Concluding this section – it would seem that in order to increase the deterrence effect of the discussed enforcement schemes on the intermediaries, harsher and more probable penalties should be implemented, together with actions taken against the intermediaries' sources of revenue originating from the transfer of infringing information.[805] That being said, there are certain factors potentially diminishing the effectiveness of such an approach. Firstly, a deterrence-oriented policy based on, for example, criminalising the operators of services related to exchange of infringing content encounters a significant difficulty when it comes to websites such as Google, Youtube, Facebook or Twitter. While those websites might often be used to spread infringing content, no prosecutor should state that arresting the operators of those

[802] And suffering sufficient detriment as a result of the said schemes' operation.
[803] For example, Tokelau and Cocos Islands, see section 2.3 of the current chapter.
[804] Schultz M, 'Copynorms: Copyright Law and Social Norms' in *Intellectual Property and Information Wealth* edited by Yu P (2007), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=933656, at 21.
[805] As to whether and how this path could be followed, see section 2.3.2.2 of chapter five.

services and confiscating their servers is in the public interest – they are too often used for the legitimate purposes.[806] Secondly, it is very difficult to distinguish between the intermediaries' profits tied to legitimate content, and profits tied to content which is infringing in nature. Nevertheless, those difficulties do not completely erase the chances of the stated twofold approach's success in enhancing the intermediary-oriented deterrence effect; and hence chapter five considers whether harsher and more probable penalties for intermediaries, together with measures aimed at the infringement-related revenue, should be endorsed as components of the recommended response to the problem of infringing content in cyberspace.

4. Diminishing returns of the enforcement schemes.

This relatively short, fourth subchapter is focused on a concept which has to be considered in the process of drafting an effective enforcement policy for the discussed area of regulation; the concept known as the law of diminishing returns. In the context of this thesis, it conveys the idea that the actual impact of the enforcement schemes on the amount of online infringing activity in cyberspace should be significant enough to justify the corresponding resources invested by the governments and the rightholders. After all, law enforcement has its costs; for example, as Danaher and Smith noted in relation to the Megaupload shutdown, "governments spend resources in order to win court cases against such sites and to mount shutdown operations"[807] – and shutting down Megaupload was certainly not a cheap endeavour.

At this point, it is worth taking note of a certain distinction between the involved content types; it is probably easier to apply the concept of diminishing returns to copyright- and trademark-infringing content than it is to

[806] Unfortunately, such charges have been pressed on certain occasions – see the Italian case of *Vividown v Google* (2014) Corte di Cassazione, sez. III Penale, sentenza n. 5107/14; depositata il 3 febbraio.
[807] Danaher and Smith, supra fn. 646, at 2.

privacy-infringing or defamatory material. With the latter two, it is more difficult to quantify the "return on the investment".[808]

There are quite a few examples which can be brought into this section in order to demonstrate how the concept of diminishing returns becomes relevant in this area of regulation. The first one is related to the idea mentioned in section 2.2 of this chapter; that the enforcement schemes aimed at online piracy should ideally be bringing about an increase in the revenue of the copyrightholders. A study conducted by Danaher et al[809] suggests the occurrence of such an increase (on the iTunes store's music sales) following the implementation of the HADOPI law. The study compared the iTunes music sales of the four major record labels before and after the introduction of the HADOPI law (data was gathered between July 2008 and May 2011), and reached the conclusion that this copyright enforcement measure was responsible for 25 % of the increase in the album sales of the control group, and 22.5 % of the increase in sales of individual music tracks.[810]

On the methodological side, the study seems to be fairly credible, despite the fact that (as the UKIPO report noted) the study only covers the (self-reported) sales of four major labels on iTunes.[811] It is quite likely that the HADOPI law moderately increased the iTunes sales in the studied period. However, the real concern is for how long it maintains this positive influence. While the Digital Britain report optimistically claims that "where there are easy, affordable and lawful routes, consumers will take them,"[812] the discussion of concerns covered in subchapter 2 leads this author to believe that once the *a priori* presumption that one has to pay for digital media is broken within the society,

---

[808] This is not to say that the debate on the impact of online piracy on the interests of copyrightholders is settled, it is far from it; Supra fn. 674, at 23.
[809] Danaher B, Smith M, Telang R, Chen S 'The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France' (2012), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989240
[810] Danaher et al, supra fn. 809, at 14.
[811] *International Comparison of Approaches to Online Copyright Infringement*, supra fn. 703, at 52.
[812] *Digital* Britain, supra fn. 690, at 110.

it never goes back to its initial shape. It is likely that those who turned to legal alternatives (such as iTunes) upon receiving a letter from the HADOPI agency are going to start looking for illegal alternatives sooner or later; and as discussed above,[813] there is a good chance that they will find them. One example confirming this presumption could be found within the Alexa's web traffic rankings. On 22nd April 2012, Uploaded.to was ranked as the 226th most popular website in the world - however, at the same time, it was the 142nd most popular website in France, and French citizens were the 4th most frequent visitors of this website.[814] The key implication of this paragraph is that when considering the law of diminishing returns, the regulators have to keep in mind the long-term perspective.[815]

Another example for this section could be derived from Friedmann's article, where he submitted that the legal interpretation of the E-Commerce Directive's safe harbours has led to a situation in which the rightholders have to continually notify the same ISSPs about the (oftentimes the same) pieces of infringing content[816] (an issue explored in section 2.1 of this chapter). Time and resources are dedicated in such a case, but it is difficult to speak of a return on the investment.

A positive example of an enforcement scheme being drawn away from the point of diminishing returns could be that of the *Newzbin 2* injunctions. As Mac Sitigh noted, the procedure for obtaining such court orders became streamlined, and thus more efficient for the rightholders and the legal system.[817] For example, in the FirstRow case,[818] the defendants did not wish to appear in court, and in fact there was no hearing; just a direct response from

[813] See section 2.2 of the current chapter.
[814] See http://www.alexa.com/siteinfo/uploaded.to
[815] (This is submitted without denying the value in the increase of sales found in the cited study.)
[816] Friedmann, supra fn. 745, at 149.
[817] Mac Sitigh D 'The fragmentation of intermediary liability in the UK' (2013) Journal of Intellectual Property Law & Practice 8(7), 521, at 522.
[818] *FAPL v Sky*, supra fn. 526

the judge. Following Meale – "(c)ompared with other court business, the process for obtaining these injunctions now appears fine-tuned".[819]

Another point of consideration is where to focus the enforcement efforts, so that the maximum possible efficiency is reached; for example, shutting down one of a hundred indexing websites might be less efficient that shutting down the cyberlocker which they are linking to. Lodder and Meulen elaborated in the similar vein: "(w)hy ask dozens, hundreds, or maybe even thousands of access providers to filter out websites if one action against the provider of the website has the same result?"[820]

To conclude – it has to be said that there is no "golden ratio", which would state that, for example, every £1,000,000 invested in an enforcement scheme should bring about a 3 % increase in the profits of the affected rightholder; nor is this thesis aiming to propose a ratio of this kind. What this section does propose is that the notion of diminishing returns is a criteria of assessment which has to be applied to policymaking in this area, and it should be further explored by corresponding empirical research containing the cost/benefits analysis of the enforcement schemes set out in chapter two. For example, as it was noted by Danaher and Smith, it would be good to know how much the operation leading to the shutdown of Megaupload cost the US taxpayers.[821]

5. Social acceptance of infringing content.

There are three primary reasons why social acceptance of the infringing content's presence in cyberspace is given its own section. Firstly, it is capable of spurring/prolifering further infringing activities in the society, and thus

[819] Meale D, 'Premier League 1, Internet pirates 0: sports streaming website the latest to be blocked' (2013) Journal of Intellectual Property Law & Practice 8(11), 821, at 822.
[820] Lodder and Meulen, supra fn. 643, at 139.
[821] Danaher and Smith, supra fn. 646, at 24.

provides a broader context to, for example, the discussion of deterrence. Secondly, focusing on the social acceptance *per se* allows for the analysis of arguments which could escape a one-sided enforcement discussion. Finally, it makes it more difficult to implement "tougher" enforcement mechanisms. Tyler wrote that in order for the law to be effective, people must believe that there is a justified moral premise behind it[822] - online content regulation became an area in which such a belief is increasingly required for the legal measures to be enacted in the first place. Lodder and Meulen remarked upon this dependence when considering legislative interventions in the copyright-infringing content area; "proposals for legislation are necessarily abstract, and likewise feel like more of a threat to the general public".[823]

It is submitted that social acceptance has been bestowed, to a lesser or greater extent, on all four types of the infringing content this thesis focuses upon. Starting with the copyright-infringing content; in the last decade, the spread of online filesharing technologies has, to an extent, given the digital media an informal status of public goods, freely accessible by anyone with a connection to the Internet. And as Schultz noted, "with the notable exceptions of oxygen bars and bottled water, it is exceedingly hard to persuade people to pay for public goods".[824] Furthermore, people who are capable of illegitimately obtaining the copyrighted material online have come to be oftentimes seen as capable individuals, granted with respect akin to that given to successful hunters in the earlier days of humanity. Trademark-infringing content is arguably less affected by social acceptance; while some individuals might be keen on obtaining fake Louis Vuitton bags through eBay, people usual prefer to avoid such counterfeit products. On the other hand, the former group's attitude indicates the presence of at least some amount of social acceptance of trademark-infringing content, acceptance which challenges the conceptual foundations of trademark law, focused traditionally on preventing the notion of confusion from taking place. Regarding privacy-infringing content, the

[822] Tyler T 'Compliance with Intellectual Property Laws: A Psychological Perspective' (1996) 29 N.Y.U. J. INT'L L. & POL. 219, at 225.
[823] Lodder and Meulen, supra fn. 643, at 138.
[824] Schultz, supra fn. 804, at 31.

erosion of privacy online and the progressing acceptance of this development (not extending to the particular rightholder whose right is/was infringed upon, of course) has been acknowledged by a fair amount of academics.[825] Finally, it is arguable that the society has grown accustomed to the fact that people regularly defame each other online in multiple ways, and (unless they happen to be the rightholder whose reputation is/was infringed upon) this fact might not be seen as a sufficient justification of the tighter regulation of the online activity.

Due to the fact that the phenomenon of social acceptance is likely to be the most present in the area of copyright-infringing content, and the fact that the community partaking in the exchange of such material is the most identifiable and distinct between the four content types,[826] the following paragraphs are going to further explore the social acceptance of this particular type of infringing content.

When one looks at the difficulties encountered by the copyright enforcement measures in cyberspace, it becomes visible that widespread copyright-infringing filesharing might be rooted in a profound social phenomenon. As Strowel argued, gathering raw data about how many people download copyright infringing material does not get us closer to understanding the community behind it.[827] Hence, this section attempts to go beyond such raw data, and explore certain aspects of the distinct (among the thesis' content areas) online community involved in copyright-infringing filesharing.

First of all, it is worthwhile to ask the following question: what happened with the social norms which could be expected to prevent the copyright-infringing

[825] See, for example, Rauhofer J 'Privacy is dead, get over it! Information privacy and the dream of a risk-free society' (2008) Information & Communications Technology Law 17(3), 185.
[826] Which also translates into the amount of relevant empirical research available.
[827] Strowel A, 'Internet Piracy as a Wake-up Call for Copyright Law Makers – Is the "Graduated Response" a Good Reply?' (2009) 1 WIPO Journal 75, at 76.

filesharers from committing acts widely known as illegal? Or, to connect this question to subchapter three and the notion of deterrence, what happened to the influence of social net utility on the infringers' decision-making process? It is possible that at least an initial part of the answer might have been revealed in the study conducted by Ingram and Hinduja in 2003, which was described in their paper from 2008.[828] The study was conducted by means of a survey administered to a group of 2,032 undergraduate students from a university in the US, and was focused on the application of the neutralisation theory to illegal filesharing. This theory was described as one explaining a situation where individuals engaging in the behaviour they know to be wrong (in this case, illegal) are "extricating themselves from personal responsibility".[829] Drawing on Sykes and Matza's seminal article from 1957,[830] Ingram and Hinduja identified four techniques of neutralisation, and conducted their survey in order to see whether they are present amongst the copyright-infringing filesharers' community.

The four techniques included: the denial of responsibility (for example, "it is not my fault that music is so expensive"), the denial of injury coupled with the denial of victim (for example, "no one will be harmed by illegal downloads, since I would not pay for them anyway"), the condemnation of the condemners (for example, "how dare they judge me, those rotten copyright industries"), and the appeal to higher loyalties (for example, "everyone should be able to enjoy this beautiful music without any limits").[831] The respondents were presented with statements representative of each neutralisation method and asked whether they agree with them, on the scale of 1 to 5.

The study found out that each of the four methods is likely to be present amongst a significant part of the illegal filesharing community, with the

[828] Ingram J and Hinduja S 'Neutralizing music piracy: an empirical examination' (2008) Deviant Behavior 29(4), 334.
[829] Ingram and Hinduja, supra fn. 828, at 338.
[830] Sykes M and Matza D, 'Techniques of Neutralization: A Theory of Delinquency' (1957) American Sociological Review 22(6), 664.
[831] Ingram and Hinduja, supra fn. 828, at 339.

overall scores ranging from 3,47 (condemnation) to 3,95 (denial of responsibility).[832] Additional evidence collected by Ingram and Hinduja disclosed that greater acceptance of the presented statements was linked to the respondent's higher downloading activity, what would be further confirming the actual application of the neutralisation methods. Finally, 90 % of the respondents regarded downloading music illegally as an appropriate behaviour overall.[833] Although the study in question was based on illegal music downloads, it is likely that its conclusions could be applied to other categories of online pirated material.

While Ingram and Hinduja's paper focused on the filesharers' individual perceptions, another study, conducted by Svensson and Larsson,[834] explored further the role of social interactions in shaping the filesharers' behaviour – a path of inquiry connected to the social net utility identified above by Watson et al.[835] A survey was administered to a group of a 1000 respondents, aged 15 to 25, which was representative in terms of both gender and the urban/rural criteria. They were given two questions; the first one was asking them to what extent do they think that people around them (for example, parents, friends, superiors) would be convinced that the respondent should not illegally download copyrighted material. The second question asked about the influence those people's opinions have on the respondent's position with regards to copyright-infringing filesharing.[836]

The main finding of this study, based on those questions, was that "no influence of social norms towards regulatory compliance"[837] was registered. While this could be partially explaining the dedicated filesharers' drive to find

[832] Ingram and Hinduja, supra fn. 828, at 345.
[833] Ingram and Hinduja, supra fn. 828, at 359.
[834] Svensson M and Larsson S, 'Social Norms and Intellectual Property. Online Norms and the European Legal Development' (2009) Research Report in Sociology of Law, vol. 1, Lund University, available at http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=1510388&fileOId=1515776
[835] See section 3.1 of the current chapter.
[836] Svensson and Larsson, supra fn. 834, at 31.
[837] Svensson and Larsson, supra fn. 834, at 45.

new sources of copyrighted material (when the ones they used are closed down), there is also another dimension of the finding in question. Those who never engaged in copyright-infringing filesharing are much more likely to step on the path of online piracy, due to the absence of social pressure to refrain from doing so – and the authors of the study notice this connection.[838] The impact of this line of reasoning and of Svensson and Larsson's study is reinforced by the findings of a survey conducted by Levin et al in 2007 on undergraduate business students,[839] as well as by the work of Watson et al, who found in their scoping review that "there was widespread evidence that the perceived beliefs and behaviors of others were correlated to individual's beliefs, intentions, and stated behaviors" related to copyright-infringing filesharing.[840]

Schultz wrote in 2006 that the gap between the social perception of online piracy and the copyright enforcement policy has to be closed, that people need to be convinced that copyright law should be obeyed.[841] However, it seems that the gap in question has become even wider since 2006, and despite the need for continuous efforts to tighten it, it is possible that the policymakers from all four content areas have to accept the existence of such gaps and devise solutions bypassing them: for example, through the removal of access to content at its source.

[838] Svensson and Larsson, supra fn. 834, at 45.
[839] Levin, A, Dato-on, M, & Manolis, C 'Deterring illegal downloading: The effects of threat appeals, past behavior, subjective norms, and attributions of harm.' (2007) Journal of Consumer Behaviour 6 (2/3), at 120.
[840] Watson et al, supra fn. 674, at 39.
[841] Schultz M, 'Fear and Norms and Rock & Roll: What Jambands Can Teach Us About Persuading People to Obey Copyright Law' (2006) 21 BERKELEY TECH. L.J. 651, at 665. To a certain extent, such a reasoning could be applied to the other three legitimate interests this thesis focuses upon.

Chapter 4 – The human rights implications of the enforcement schemes' activity.

1. Introduction.

In the pursuit of effective enforcement schemes, the regulators should not forget that there is a rich layer of human rights permeating the discussed area of law. Some of them stand behind the enforcement schemes identified in chapter two, while others are threatened by their operation. This leads to the inevitable clashes between those two sets of human rights, and in consequence, the need to balance them out with each other.[842] When looking for the most adequate legal framework governing the removal of access to the identified types of infringing content, it is absolutely crucial to consider the human rights perspective.

As it might be apparent after the mention of the "need to balance" in the previous paragraph, this chapter is fundamentally different from its predecessor. The third, effectiveness-oriented chapter was fairly one-dimensional, effectiveness being the only angle of assessment, the only goal sought. The fourth chapter does not endorse a singular, vertical notion of "compatibility with human rights", because it is impossible to do so, due to the earlier mentioned fact that some of them support the enforcement schemes, while the others might be hindered by such measures. Instead, this part of the thesis is focused on analysing in detail the nature of the conflict areas arising between the involved human rights, and on discovering how courts and regulators set the balance between those rights.

[842] It should be noted that the human right behind an enforcement scheme and the human right threatened by the said scheme do not have to be two different rights; see section 3.1 of the current chapter.

In order to achieve the earlier mentioned aims, the current chapter adopts the following structure, consisting of two primary subchapters. The first one (section 2) introduces the key human rights influencing this area of law, namely the right to property (section 2.1), the right to respect for private and family life (section 2.2), the freedom of expression and information (section 2.3), the freedom to conduct a business (section 2.4), and the right to an effective remedy and to a fair trial (section 2.5).

The second subchapter (section 3) explores the key conflict areas between the involved human rights, through a set of three sections, each of them pitting the human rights supporting the four legitimate interests this thesis focuses upon with one of the three human rights which are at risk of being impaired by the enforcement schemes; this being the right to respect for private and family life (section 3.1), the freedom of expression and information (section 3.2), and the freedom to conduct a business (section 3.3).

2. The relevant human rights.

Before this section begins to outline and discuss the key human rights involved in this area, a crucial preliminary question has to be answered; which document(s) is this thesis going to use as the source of the definitions of said human rights? The European Convention on Human Rights (hereafter referred to as the ECHR), as interpreted by the European Court of Human Rights (hereafter referred to as the ECtHR)? The Charter of Fundamental Rights of the European Union (hereafter referred to as the CFREU), as interpreted by the Court of Justice of the European Union (hereafter referred to as the CJEU)? The Universal Declaration of Human Rights (hereafter referred to as the UDHR)? Given the EU focus of this thesis, it is useful to answer this question with reference to art. 6 of the Treaty on the European Union (hereafter referred to as the TEU). Art. 6(3) of the TEU states that "(f)undamental rights, as guaranteed by the European Convention for the

Protection of Human Rights and Fundamental Freedoms [the ECHR] and as they result from the constitutional traditions common to the Member States, shall constitute *general principles* of the Union's law".[843] On the other hand, art. 6(1) of the TEU provides that "(t)he Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have *the same legal value as the Treaties*".[844]

Therefore, after analysing the cited provisions,[845] the thesis adopts the CFREU as the primary source of the human rights' definitions, with the relevant CJEU rulings continuing to be of highest authority value throughout the chapter. The ECHR and the ECtHR case law are relied on as close points of reference and guidance in both subchapters 2 and 3, their value augmented by the potential accession of the EU to the ECHR.[846] Finally, the provisions of the UDHR, as well as of the International Covenant on Civil and Political Rights (hereafter referred to as the ICCPR), and International Covenant on Economic, Social and Cultural Rights (hereafter referred to as the ICESCR) are sparsely cited in the current subchapter, as points of comparison to the definitions of the CFREU. Giving the illustrated priority to the Charter could be seen as further supported by a quote from the Advocate-General Cruz Villalón in *Scarlet*: "(…) the rights, freedoms and principles stated in the Charter have, in themselves, a legal value which, furthermore, is of the highest level".[847]

It should be noted that there are certain human rights which bear some links to the discussed area of law, but have not gained sufficient presence to be distinguished in the same manner as the cited five. The former include the freedom of association,[848] the right to participate in the cultural life of the

[843] Treaty on the European Union, art. 6(3), emphasis added.
[844] TEU, supra fn. 843, art. 6(1), emphasis added.
[845] (And as some of the keen-eyed readers might have noticed from the endorsed names of human rights mentioned in the introduction to this subchapter.)
[846] See http://www.echr.coe.int/Pages/home.aspx?p=court/accessioneu&c.
[847] Opinion of AG Cruz Villalón in the Case C-70/10, supra fn. 539, at [30].
[848] Set out in art. 12 of the CFREU.

society[849] and the right to education.[850] Freedom of association could be of relevance in a situation where, for example, an online forum used (among others) for sharing infringing content is shut down by the police. Users of the said forum could argue that they are not allowed to congregate in this virtual environment. The right to participate in the cultural life of the society might be seen as a source of support for, for example, poverty-stricken copyright infringers wishing nevertheless to take part in their community's cultural life. Finally, people such as students downloading textbooks in breach of copyright could try to rely on the right to education in their defence.

Lastly, it is worth noting here that as much as the human rights are enshrined in the cited documents, the development of technology is one of the factors which may alter the scope or even the core of the said rights, <>given enough time. As Hert and Kloza wrote, "(…) one does equally not need to be too fundamentalist about fundamental or human rights either. These rights are not holy and are far from static. They evolve, simply because they reflect developments in the society, rather than eternal truths or state of beings of human kind".[851] Freedom of expression, covered in section 2.3 of the current subchapter, stands as a testimony to this view of human rights.

2.1. The right to property.

The right to one's property is covered first, as it stands behind the online enforcement schemes aimed at tackling both copyright-infringing and trademark infringing content, which are the first two interests this thesis focuses upon. It is defined in art. 17(1) of the CFREU, which states that: "(e)veryone has the right to own, use, dispose of and bequeath his or her lawfully acquired possessions. No one may be deprived of his or her

[849] Set out in art. 27 of the UDHR.
[850] Set out in art. 14 of the CFREU.
[851] De Hert P and Kloza D, 'Internet (access) as a new fundamental right. Inflating the current rights framework?', European Journal of Law and Technology, Vol. 3. No. 3, 2012, at 2.

possessions, except in the public interest and in the cases and under the conditions provided for by law, subject to fair compensation being paid in good time for their loss. The use of property may be regulated by law in so far as is necessary for the general interest".[852] As it will be shown in subchapter 3, the reference to regulation in the name of general interest (or its various forms) does come into play on quite a few occasions in this area of law.

Furthermore, as it was mentioned in section 2.1 of the first chapter, the right to property is expressly expanded in the CFREU to cover intellectual property; art. 17(2) straightforwardly states "intellectual property shall be protected".[853] It is quite significant that the said type of property is the only one to receive such special treatment in the Charter; art. 17(2) seems to be indicating how high the protection of IP stands/stood for the EU policymakers.

As for the ECHR, art. 1 of the first Protocol to the Convention states that "every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law".[854] And also: "(t)he preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties".[855] No express mention is given to the intellectual property.

The UDHR also sets out the right to property in art. 17: its section (1) provides that "everyone has the right to own property alone as well as in association with others",[856] with section (2) stating that "no one shall be arbitrarily

[852] CFREU, supra fn. 7, art. 17(1).
[853] CFREU, supra fn. 7, art. 17(2).
[854] ECHR, supra fn. 173, art. 1 of Protocol 1.
[855] ECHR, supra fn. 173, art. 1 of Protocol 1.
[856] UDHR, supra fn. 172, art. 17(1).

deprived of his property".[857] ICESCR and ICCPR do not contain an express human right to property. However, two out of the three instruments cited in this paragraph do bestow the human rights' status on the protection of copyright, separating it here from the protection of trademarks. Art. 27(2) of the UDHR declares that "everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author".[858] Similarly, art. 15(1)(c) of the ICESCR asserts that "the States Parties to the present Covenant recognize the right of everyone: (…) (t)o benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author".[859]

Sections 2.2 and 3.2 of the first chapter present a wide selection of ways in which the human right set out in art. 17 of the CFREU can be infringed by means of online content.

2.2. The right to respect for private and family life.

As it was laid out in section 4.1 of chapter one, the right to respect for private and family life underlies the legitimate interest threatened by the privacy-infringing content; though as subchapter 3 is going to demonstrate, this human right can also be found on the other side of the dispute, with enforcement schemes threatening the privacy of some of the involved stakeholders, most commonly the original infringers.[860]

Section 2.1 of the first chapter set out the three key incarnations of the right to privacy (present in the CFREU, the ECHR and the UDHR); it is worth

[857] UDHR, supra fn. 172, art. 17(2).
[858] UDHR, supra fn. 172, art. 27(2).
[859] International Covenant on Economic, Social and Cultural Rights, art. 15(1)(c).
[860] See section 3.1 of the current chapter.

bringing them back in this section. Therefore; art. 7 of the CFREU states that "everyone has the right to respect for his or her private and family life, home and communications",[861] with art. 8 of the ECHR almost mirroring this provision by declaring that "everyone has the right to respect for his private and family life, his home and his correspondence".[862] Art. 12 of the UDHR asserts that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".[863] As for the ICCPR, its art. 17 mirrors the described provision of the UDHR, save for adding the word "unlawful" to the interference in question.[864] The ICESCR does not set out an express right to privacy.

The right to respect for private and family life contains two, arguably derivative aspects which are relevant to the discussed area of law; the first one being the right to data protection. As much as some of the more recent interpretations of this right could be seen as having moved away from its privacy-based conceptual underpinnings,[865] this author is of the opinion that protection of personal data should be regarded as a means to safeguarding people's privacy, not as an end in itself. The CJEU in *Promusicae* adopted an approach compatible with this position, in regarding the right to protection of personal data as an extension of the right to privacy.[866]

Nevertheless, it has to be admitted that this matter is far from settled. As Lynskey writes, "the relationship between these two rights is contested, with some arguing that data protection is merely a subset of the right to privacy

[861] CFREU, supra fn. 7, art. 7.
[862] ECHR, supra fn. 173, art. 8.
[863] UDHR, supra fn. 172, art. 12.
[864] International Covenant on Civil and Political Rights, art. 17(1) and (2).
[865] Leading to certain judicial decisions which are difficult to justify, for example, that of the CJEU in Case C-131/12 *Google Spain v Gonzalez*.
[866] *Promusicae*, supra fn. 322, at [63].

while others advocate that it is an independent right".[867] Elucidating the point, the cited author argues that while the UK is traditionally closer to the former position (due to, for example, the case of *Durant*[868]), countries such as Germany rather embrace the latter, with the notion of 'informational self-determination' regarded as the base of data protection.[869] Furthermore, the CJEU judgement in *Costeja* can be perceived as providing "implicit support for the recognition of 'individual control over personal data', irrespective of whether these personal data are 'private', as a fundamental aspect of the right to data protection."[870] And it remains a fact that data protection was granted its own place in the CFREU; as it was mentioned in section 4.1 of chapter one, art. 8 of the Charter provides that "everyone has the right to the protection of personal data concerning them".[871] Finally, similarly to the protection of intellectual property, one could say that data protection received a significant amount of favour from the EU policymakers; as Tsoutanis noted, not without a sense of humour; in CFREU, "(…) the protection of 'personal data' precedes other fundamental rights, such as the 'right to marry' and 'freedom of thought and religion.' This is probably as good as it gets. Privacy trumps God".[872]

Nonetheless, this author retains the opinion that the right to privacy "umbrella" is a fitting shelter for data protection, diminishing the latter's chances of becoming unjustifiably expanded and harmful to freedom of expression and other legitimate interests.

The second relevant extension of the right to privacy is its aspect of the human right standing behind the protection of reputation. Introduction to chapter one stated that defamation law is not harmonised on the EU level; and this still holds true. However, in the human rights realm, a certain twist appears and the

[867] Lynskey O, 'Control over Personal Data in a Digital Age: *Google Spain v AEPD and Mario Costeja Gonzalez*' (2015) 78(3) MLR 522–548, at 529.
[868] *Durant v Financial Services Authority* [2003] EWCA Civ 1746 at [28] per Auld LJ.
[869] Lynskey, supra fn. 867, at 529.
[870] Lynskey, supra fn. 867, at 529.
[871] CFREU, supra fn. 7, art. 8.
[872] Tsoutanis, supra fn. 324, at 952.

defamatory content may be regarded as a threat to the right to respect for private and family life. This stance has been adopted on many levels of the legal debate at hand. Firstly, the cited definitions of the right to privacy set out in the UDHR and the ICCPR extend the protection to attacks on "honour or reputation". Secondly, in the ECtHR case of *Delfi v Estonia* (2013), the Court reiterated that "the right to protection of reputation is a right which is protected by Article 8 of the Convention as part of the right to respect for private life".[873] Furthermore, the UK House of Lords' case of *In re British Broadcasting Corporation* (2009) interpreted the right to privacy (set out by the same article) as covering the injury to the person's reputation.[874] And for the final example, Bennett argued in his article that it is strange that in the case of *Applause Store*,[875] the damages awarded in defamation were far higher than those awarded for the breach of privacy, as "the Convention [ECHR] right which is engaged is the same for both claims--Art.8".[876] While on the conceptual level, it could be argued that defamation should not be regarded as going against the right to privacy (especially if we consider the classic English definitions from *Sim v Stretch*[877] or *Yousoupoff v MGM Pictures*[878]), this work is not aimed at exploring this issue and accepts the right to respect for private and family life as the human right protecting the reputation of the EU citizens.

2.3. The freedom of expression and information.

In the ECtHR case of *Kulis v Poland* (2009), freedom of expression was characterised as "one of the essential foundations of a democratic society".[879] It has to be admitted that when it comes to defining the scope, this particular foundation is an exceptionally challenging one. Not to say that freedom of expression is alone here; most of the human rights encounter difficult

[873] (2013) Application no. 64569/09, at [80].
[874] [2009] UKHL 34, at [22].
[875] Supra fn. 233, case covered in section 5.2.4 of chapter one.
[876] Bennett T, 'Horizontality's new horizons - re-examining horizontal effect: privacy, defamation and the Human Rights Act: Part 1' (2010) Ent.L.R. 21(3),at 103.
[877] *Sim v Stretch*, supra fn. 210.
[878] *Yousoupoff v MGM Pictures*, supra fn. 211.
[879] (2009) Application 27209/03, at [28].

questions about their reach. However, the right covered in this section stands out when questions such as "what kind of expressions should be covered by the freedom of expression?" and "should any categories of expression be granted a higher level of protection than others?" are being asked.

To give a taste of the debate behind such questions; according to Brown and Waelde, the courts might be inclined to decide that "political speech should be accorded most weight when considering claims of freedom of expression, with intellectual, educational and artistic, and then commercial, speech following thereon".[880] However, as Helfer and Austin wrote, "informed political participation (…) requires access to information, such as news reports and other media".[881] Defining the kinds of information required for informed political participation is an exceedingly difficult exercise, as people's choices might be influenced by an immense amount of content types, many of them not being infused with the political flavour; and this is just one of the scope-related dilemmas this human right encounters.

Returning to the main analytical stream of this chapter; after setting out the relevant legal framework, this section is going to discuss three possible, thesis-relevant expansions of the freedom of expression's scope.

Art. 11 of the CFREU states that "(e)veryone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers".[882] As for the ECHR, its art. 10(1) mirrors the cited provision in full.[883] The following art. 10(2) is worthy of being cited in full, as it declares that "the exercise of these freedoms, since it carries with it duties

[880] Brown A and Waelde C, 'A practical analysis of the human rights paradox in intellectual property law: Russian Roulette', in Grosheide W (ed) Intellectual Property and Human Rights: A Paradox (2010), at 201.
[881] Helfer L and Austin G *Human Rights and Intellectual Property: Mapping the Global Interface* (2011), at 221.
[882] CFREU, supra fn. 7, art. 11.
[883] ECHR, supra fn. 173, art. 10(1).

and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the *protection of the reputation or rights of others*, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary".[884] This provision is crucial to the reasoning behind the ECtHR case law discussed in this chapter.

Looking towards the UDHR, we find art. 19, which provides that "everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to *seek*, receive and impart information and ideas through any media and regardless of frontiers".[885] It is worth to give attention here to the inclusion of the word "seek", which in the era of multiple types of indexing services might come to provide for a crucial difference between the UDHR and the first two instruments covered in this section. As for the ICCPR, it follows UDHR in this regard, by stating in its art. 19 that "everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice".[886] The ICESCR does not contain a provision setting out the general freedom of expression.

There are three particularly relevant ways in which the scope of freedom of expression could be expanded; while they are not as established as the extensions of the right to privacy, (covered in the previous section) it still seems plausible to discuss them before the chapter moves into its rights-balancing phase. Firstly, just as the right to data protection was described in section 2.2 as a means to protect the broader right to privacy, so can the freedom of expression be seen as a means to enabling the right to participate in

[884] ECHR, supra fn. 173, art. 10(2), emphasis added.
[885] UDHR, supra fn. 172, art. 19, emphasis added.
[886] ICCPR, supra fn. 864, art. 19(2).

the cultural life of the society. The definition of the latter can be found in art. 27(1) of the UDHR, which proclaims that "everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits".[887] Additionally, art. 15(1)(a) of the ICESCR requires the signatories of this instrument to "recognize the right of everyone (…) to take part in cultural life",[888] with art. 15(3) obliging the said signatories to "respect the freedom indispensable for scientific research and creative activity".[889]

The second potential expansion could be drawn towards the protection of broadly understood innovation. The 7th of the 10 Internet Rights and Principles (compiled in a legally non-binding document created by the UN's Internet Governance Forum) provides that the "(…) technical and policy innovation should be encouraged to facilitate plurality of expression".[890] This connection, drawn between innovation and the freedom of expression, seems to be a plausible one, with the former concept propelling and facilitating the latter. Furthermore, this line of reasoning could be seen as being supported by the ECtHR decision in *Neij and Sunde Kolmisoppi v Sweden* (2013), where it was asserted that "(a)rticle 10 [of the ECHR] applies not only to the content of the information but also to the means of transmission or reception since any restriction imposed on the means necessarily interferes with the right to receive and impart information".[891] The development and operation of new, diverse and more efficient methods of exchanging information in cyberspace could accordingly be seen as protected by the freedom of expression.

The last interpretative extension to be explored in this section surrounds the notion of the hypothetical right of access to the Internet being covered by the freedom of expression; this connection is one of the variants explored in Hert

[887] UDHR, supra fn. 172, art. 27(1).
[888] ICESCR, supra fn. 859, art. 15(1)(a).
[889] ICESCR, supra fn. 859, art. 15(3).
[890] Internet Governance Forum, *The Charter of Human Rights and Principles for the Internet* (2014) 3rd ed, at 7.
[891] (2013) ECtHR, application no. 40397/12, at 9.

and Kloza's article analysing various forms which the said right of access to the cyberspace could take.[892] Frank la Rue, the UN Special Rapporteur on the freedom of expression, stated in 2011 that "the Internet has become an indispensable tool for realizing a range of human rights".[893] Taking this quote further, one could argue that, as the Internet is, at its core, an immense system for "receiving and imparting" information, the right of access to the Internet could be seen as (inter alia) enabling the freedom of expression (which in turn, could be seen as (inter alia) enabling a "range of human rights" mentioned by the Rapporteur). While Hert and Kloza ultimately argue in favour of introducing a stand-alone human right of access to the Internet,[894] which would be independent of the freedom of expression, this thesis lacks the time and space to discuss the merits of such a proposition. Instead, it is accepted that the latter right could be seen as covering the former, which opens up a valuable analytical perspective for section 3.2.

2.4. The freedom to conduct a business.

The freedom to conduct a business is a relatively new human right, but in recent years, it has started to gain ground as an important element of the debate surrounding online content regulation. It is set out in art. 16 of the CFREU, which states that "the freedom to conduct a business in accordance with Community law and national laws and practices is recognised".[895] It is worth noting how modest the phrasing of this article is; the use of the term "recognition" could be compared with a much more assertive "no one shall be deprived of (…)" (art. 1 of the Protocol 1 of the CFREU) or "the right to respect (…)" (art. 7 of the CFREU).

[892] Hert and Kloza, supra fn. 851.
[893] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, at 85, available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
[894] Hert nad Kloza, supra fn. 851, at 12.
[895] CFREU, supra fn. 7, art. 16.

The ECHR and UDHR do not contain provisions setting out a human right corresponding to the one covered in this section. Neither does the ICCPR or the ICESCR, though a significantly extensive reading of their arts. 1(1) (which state that "(a)ll peoples have the right of self-determination. By virtue of that right they freely determine their political status and freely pursue their *economic*, social and cultural *development*"[896]) could indicate this provision as indirectly supporting the freedom to conduct a business.

2.5. The right to an effective remedy and to a fair trial.

The last human right to be presented in this subchapter is the right to an effective remedy and to a fair trial. In contrast to the previous four, it is less tied to a specific legitimate interest and is more of a concept which permeates through the area of online content regulation. Hence, while it is not a side in any of the balancing exercises conducted in subchapter 3, it remains one of the key human rights which the policymakers should keep in mind when looking for an adequate response to the challenge of infringing content in cyberspace.

In CFREU, it is set out in art. 47, which states, firstly, that "(e)veryone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article"[897] and secondly, that "(e)veryone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law (…)".[898]

The ECHR splits effective remedy and fair trial into two separate provisions; firstly, art. 6 of the Convention declares that "(i)n the determination of his civil rights and obligations or of any criminal charge against him, everyone is

[896] Supra fns. 859 and 864, emphasis added.
[897] CFREU, supra fn. 7, art. 47.
[898] CFREU, supra fn. 7, art. 47.

entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. (…)"[899] Secondly, art. 13 provides that "(e)veryone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity".[900]

A similar division is endorsed by the UDHR, art. 8 of which states that "(e)veryone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law",[901] with art. 10 asserting that "(e)veryone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his rights and obligations and of any criminal charge against him".[902] The ICCPR also divides the two rights; firstly, art. 2(3) obliges the signatories "(t)o ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity".[903] Secondly, art. 14(1) states that "(a)ll persons shall be equal before the courts and tribunals. In the determination of any criminal charge against him, or of his rights and obligations in a suit at law, everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law".[904] The ICESCR does not contain corresponding provisions.

There is one possible interpretative expansion of the right set out in art. 47 of the CFREU worth bringing up in the current section, tied to the notion of transparency. This concept reflects the value of maintaining a clear and publicly open lawmaking process, as well as implementing the adopted laws in

[899] ECHR, supra fn. 173, art. 6.
[900] ECHR, supra fn. 173, art. 13.
[901] UDHR, supra fn. 172, art. 8.
[902] UDHR, supra fn. 172, art. 10.
[903] ICCPR, supra fn. 864, art. 2(3)(a).
[904] ICCPR, supra fn. 864, art. 14(1).

a similar manner. Following this path can be seen as a way of improving the social acceptance of enforcement schemes, as well as decreasing the chance of laws being inappropriately influenced by the involved stakeholders. The area of online content regulation suffered from quite a few shortcomings in this regard (especially in the copyright context), and the reference to a "fair and public hearing" conducted by an "independent and impartial tribunal" seems to be spiritually accommodating the value of transparency.

3. Balancing the involved human rights.

As it was indicated in the introduction to this chapter, none of the human rights outlined in subchapter 2 is absolute; on occasions of conflict, they have to be balanced with each other. In the EU, this position is upheld by art. 52(1) of the CFREU, which states that "(a)ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union *or the need to protect the rights and freedoms of others*".[905]

Lord Steyn's judgement in the *Re S* (2003)[906] case set out four principles aimed at guiding the act of balancing arts. 8 and 10 of the ECHR with each other; however, it is submitted (in accordance with the line of reasoning given in *Golden Eye v Telefonica* (2012)[907]) that those principles could be expanded to cover all human rights paired up in the current subchapter. The principles in question, which are embraced by this thesis, were stated as follows:

- "First, neither article has precedence over the other.
- Secondly, where the values under the two articles are in conflict, an

[905] CFREU, supra fn. 7, art. 52(1), emphasis added.
[906] [2004] UKHL 47.
[907] [2012] EWHC 723 (Ch), at [117].

intense focus on the comparative importance of the specific rights being claimed in the individual case is necessary.

- Thirdly, the justifications for interfering with or restricting each right must be taken into account.
- Finally, the proportionality test[908] must be applied to each".[909]

3.1. The four protected interests vs the right to respect for private and family life.

3.1.1. Disclosing the infringers' details to the rightholders.

The first major area in which the four legitimate interests lying at the heart of this thesis come into conflict with the right to respect for private and family life is the notion of rightholders seeking to obtain the personal details of online infringers from the intermediaries. To provide content-specific examples: this conflict area arises whenever a copyrightholder wishes to identify an infringer who uploaded the former's copyrighted movie onto a cyberlocker, a trademark owner requests the disclosure of a counterfeit trader's data, a movie star seeks to locate the infringer who uploaded the former's private nude pictures, or an owner of a defamed company tries to locate the online defamer.

The primary tool on which the rightholders rely to acquire the discussed information is a judicial order obliging the intermediary to disclose the requested data. As Collingwood wrote about such orders (in the privacy context); they "may facilitate the identification of a wrongdoer who may then ultimately be pursued through the courts, but they should not be undertaken lightly, particularly because revealing the details of an individual expecting to

[908] Characterised by Lord Steyn as the "ultimate balancing test".
[909] *Re S*, supra fn. 906 at [17].

rely on the protection of anonymity clearly has major data protection issues, due to their intrusive nature".[910] The right to data protection's presence in the discussed circumstances is all too clear.

Therefore, we encounter a conflict between the four identified legitimate interests, and the right to privacy (primarily in its aspect of the right to data protection). How then has the EU legal framework and its courts balanced those human rights in the discussed context?

Generally, it can be said that the rightholders' efforts aimed at identifying infringers prevail over the latter's right to privacy. This submission is supported first and foremost by the identification-enabling legislative provisions discussed in section 2.3 of chapter two, such as arts. 6(b) and 15(2) of the E-Commerce Directive,[911] as well as art. 8(1) of the Enforcement Directive[912] (when copyright and trademarks are considered). Furthermore, the numerous occasions on which the copyrightholders were successful in obtaining the disclosure orders in question further reinforces the described perception. Taking the UK as an example, the so-called *Norwich Pharmacal* (1974)[913] orders, warranting the identity disclosure requests aimed at parties who became involved in the tortious activities of a third party,[914] are regularly used against individuals spreading infringing content; *Polydor v Brown*[915] being one of the examples demonstrating such usage, the disputable activity of law firms such as ACS:Law[916] being another.

Moving further in this line of inquiry towards copyright specifically, we once again encounter the CJEU case of *Promusicae*.[917] As it might be remembered

[910] Collingwood, supra fn. 245, at 4.
[911] E-Commerce Directive, supra fn. 91.
[912] Enforcement Directive, supra fn. 247.
[913] [1974] A.C. 133.
[914] *Norwich Pharmacal*, supra fn. 913, at 205.
[915] *Polydor v Brown*, supra fn. 129, covered in section 2.2.3.3. of chapter one.
[916] Covered in section 2.1.1 of chapter two.
[917] *Promusicae*, supra fn. 322.

from section 2.3 of the second chapter, the Court stated that, while the relevant provisions of EU law do not oblige the Member States to establish an intermediary's duty to "communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings", they also do not prevent Member States from introducing such obligations. In reaching this decision, the CJEU considered the human rights pairing of copyright vs. privacy, underlining the importance of giving attention to "(…) the need to reconcile the requirements of the protection of different fundamental rights, namely the right to respect for private life on the one hand and the rights to protection of property and to an effective remedy on the other".[918] Following this case, there is little doubt that the policymakers within the EU considering the current and future identification procedures aimed at online copyright infringers have to give attention to the right to privacy; though it does not preclude them from setting the balance in favour of the copyrightholders in the discussed context. Given the reference to the "right to property" this conclusion could extend to trademarks as well.

Aside from considering the legal requirements for the disclosure of the infringer's personal data, it is also worth thinking about what data is or should be collected by the intermediaries and made available upon successful rightholders' requests. A particularly relevant case which dealt with this matter is the CJEU decision in the *Seitlinger* (2014)[919] case, which invalidated the Data Retention Directive[920] on the basis of the latter's incompatibility with art. 7 of the CFREU. Art. 5 of the directive set out various categories of data which were to be retained by the relevant intermediaries; this included, among others, "data necessary to trace and identify the source of a communication"[921] (for example, users' IDs, IP addresses), "data necessary to identify the

[918] *Promusicae*, supra fn. 322, at [65].
[919] Case C-293/12 *Digital Rights Ireland Ltd v Seitlinger* (2014).
[920] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
[921] Data Retention Directive, supra fn. 920, art. 5(a).

destination of a communication"[922] (for example, also users' IDs and IP addresses), and "data necessary to identify the type of communication"[923] (for example, type of online service used). The obligation to collect such data was regarded in itself as "an interference with the rights guaranteed by Article 7 of the Charter".[924] It was stated that "those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them".[925] Hence, following this decision, the content of the data pond from which the European rightholders might want to "fish out" the infringers' details might be difficult to predict, as the requirements vary from one Member State to another.

One of the side elements of the balancing exercise (prompted by the discussed identification attempts) deserves to be flagged up here: namely, the cost element. Effective identification procedures might take up quite a lot of the rightholder's resources (whether we consider the *Norwich Pharmacal*-style injunctions or the graduated response schemes[926]), especially if we are dealing with a situation involving a huge number of alleged infringers and/or a small-scale rightholder. For example, Tsoutanis submitted in 2013 that "(i)n practice, getting ISPs to identify their customers often involves much uncertainty, high cost and significant delays for everybody involved".[927] While the actual efficiency of the said identification efforts remains a subject for empirical examination, such criteria should be incorporated into the balancing exercise at hand, for all four content types.

[922] Data Retention Directive, supra fn. 920, art. 5(b).
[923] Data Retention Directive, supra fn. 920, art. 5(d).
[924] *Seitlinger*, supra fn. 919, at [34].
[925] *Seitlinger*, supra fn. 919, at [27].
[926] Covered in section 2.4 of chapter two.
[927] Tsoutanis, supra fn. 324, at 954.

In its Communication from 2002, entitled *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, the European Commission stated that "the possibility of remaining anonymous is essential if the fundamental rights to privacy and freedom of expression are to be maintained in cyberspace".[928] It is quite clear that while certain crucial questions remain to be answered (for example, how much evidence of infringement should be required to obtain a disclosure order? How grave should the infringing activity be?), the legal systems functioning within the EU legal framework are definitely prepared to dismiss the users' anonymity for the sake of the relevant legitimate interests. Given the potential future growth of, for example, the decentralised, anonymity-focused P2P networks, the policymakers should start thinking on how the status of the described human rights pairing should be adapted to factual scenarios in which the disclosure orders are redundant, due to the lack of a targetable online intermediary.

3.1.2. Filtering measures affecting the online users' privacy.

In addition to the identification measures, the use of content filtering schemes prompted the appearance of another major arena on which the four interests and the right to respect for private and family life clash. In this instance, the interference might occur whenever the users' data is scanned for infringing content, making the former type of information susceptible to being accessed by third parties (especially when deep packet inspection[929] is in use), or whenever the filtering system gathers data such as logs demonstrating the users' online activities.

---

[928] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime – eEurope* 2002 (COM(2000) 890 final, at 20.

[929] Which can be defined as "(…) a technology deployed at the level of Internet provision to decipher the content of the information that is travelling through the network", *per* Daly A, 'The legality of deep packet inspection' (2011) I.J.C.L.P. 14, at 2. For further discussion of this method of filtering see section 2.3.1.2 of chapter five.

The first crucial CJEU decision which dealt with this kind of a threat to the right to respect for private and family life was made in the copyright case of *Scarlet Extended*.[930] As it might be remembered from section 3.1.2.3.1 of chapter two, the right to data protection was one of the three human rights factors which led the Court to dismiss the filtering system which was endorsed by the Belgian Court of Appeal. The judges of the CJEU stated that "(i)t is common ground, first, that the injunction requiring installation of the contested filtering system would involve a systematic analysis of all content and the collection and identification of users' IP addresses from which unlawful content on the network is sent. Those addresses are protected personal data because they allow those users to be precisely identified".[931] Additionally, it is worth bringing attention here to the opinion of the Advocate General in this case, who noted that the requested filter would cover not only the information of Scarlet's customers, but also that of other online users communicating with the former group:[932] thus further encroaching upon the right to data protection and the right to respect for private and family life. Angelopoulos characterised the filtering order in *Scarlet* as "strikingly broad"[933] – and this opinion receives further support in the following paragraphs.

The second judgment of the CJEU which receives this section's attention is the Court's decision in the earlier mentioned copyright case of *Netlog*,[934] where a different filtering injunction was dismissed on the basis of, *inter alia*, its impact on the right to respect for private and family life. As it might be remembered, instead of an ISP whose services are used for P2P infringement (*Scarlet*), the *Netlog* case concerned a social network, the users of which were sharing copyrighted material through the platform. Consequently, the filtering system requested by SABAM was characterised by the Court as one aimed at

[930] *Scarlet Extended v SABAM*, supra fn. 105.
[931] *Scarlet Extended v SABAM*, supra fn. 105, at [51].
[932] Supra fn. 539, at [59].
[933] Angelopoulos C, 'Are blocking injunctions against ISPs allowed in Europe? Copyright enforcement in the post-Telekabel EU legal landscape' (2014) Journal of Intellectual Property Law & Practice, Vol. 9, No. 10 , at 814.
[934] *SABAM v Netlog*, supra fn. 103.

hosting providers, obliging them to conduct filtering of information which is stored on their servers by their service's users, in the form covering all those users indiscriminately, as a preventative measure, exclusively at the hosting providers' expense and for an unlimited period.[935]

CJEU stated that such a filtering scheme would also be interfering with the right to data protection: though in a slightly different manner than in *Scarlet Extended*. It was proclaimed that "the injunction requiring installation of the contested filtering system would involve the identification, systematic analysis and processing of information connected with the profiles created on the social network by its users. The information connected with those profiles is protected personal data because, in principle, it *allows those users to be identified*".[936] When seen together with the impact of the filtering system in question on the freedom to receive or impart information and the freedom to conduct business, this interference with the right to data protection was regarded as an unjustifiable one, failing to strike the right balance between the human rights involved.[937]

Finally, it is worth mentioning here another excerpt from the AG's opinion in *Scarlet*, in which he referred to the ECtHR case of *Copland v UK* (2007), where it was held that "the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and Internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8".[938] Accordingly, a filtering system which would be gathering logs describing users' activity in cyberspace would also be likely to encounter a significant challenge from the side of rights protected under arts. 7 and 8 of the CFREU.

[935] *SABAM v Netlog*, supra fn. 103, at [26].
[936] *SABAM v Netlog*, supra fn. 103, at [49], emphasis added.
[937] *SABAM v Netlog*, supra fn. 103, at [51].
[938] (2007) Application no. 62617/00, at [44].

Although *Scarlet* and *Netlog* are both copyright cases, it is submitted in this section that their conclusions on the filtering systems' interference with the right to respect for private and family life can be seen as applying across all four content types. This is because while various content-specific filters might be focused on different elements of information (for example, a keyword filter vs. an image-based one), the decisions cited above are focused on the ways in which privacy might be infringed, as opposed to being tied to copyright-infringing content. As for the case of *Copland*, while it did not concern infringing content in cyberspace, the privacy-infringing practices described in the cited passage can find their way into the realm of filtering schemes; hence, this passage can be seen as a piece of guidance for all four content-type areas.

To conclude; it seems that filtering systems carrying a significant risk of interfering with the online users' privacy (by, for example, being based on a systematic analysis of content, collecting IP addresses and other personal data, and/or operating in an indiscriminate manner) might be less likely to receive acceptance from the CJEU and which follows, from the EU law. On the other hand: filters which are less invasive on privacy, which are narrower and more precise in their interference, might come to be accepted on the European stage. One thing is certain: the policymakers in this area have to keep a track of the developments in the filtering technologies, in order to be able to properly assess – inter alia - their impact on the users' right to privacy.

3.1.3. Infringement of privacy resulting from the responsibility for third parties infringing through the online user's connection.

This is a fairly old concern, related to a situation in which one party might be held responsible for the infringements conducted by others through the former's Internet connection; this could be students infringing copyright through their university's wires, or children sharing similar content through their parents' online connection. In her article on the Digital Economy Act

2010, Edwards expressed the arising concern, submitting that in order to avoid liability, the connection owners might be compelled to supervise or even police the online behaviour of those who use their connection: which (depending on the manner of such supervision) might lead to a threat to the latter's right to privacy.[939]

While this point was made in the context of the graduated response, there is no reason why it should not be considered in relation to all other relevant, infringer-focused enforcement schemes. Additionally, it can also be seen as applicable to all four content types; while children and university students are likely to try to obtain a new movie for free, they might also sell counterfeit products on auction sites, or release privacy-infringing and defamatory materials on social media websites.

3.2. The four protected interests vs the freedom of expression and information.

Before focusing on the specific conflict areas of this section, it is worth remarking upon a set of interesting, conceptual correlations arising between the freedom of expression and copyright specifically. As it was stressed in *Scarlet*, "the protection of the fundamental right to property, which includes the rights linked to intellectual property, must be balanced against the protection of other fundamental rights".[940] When we consider copyright, one of the most crucial rights of the latter category is the freedom of expression. These two rights are inseparably linked from the very beginnings of copyright, and the various views on the nature of this pairing deserve to be presented and discussed here.

[939] Edwards, supra fn. 361, at 536.
[940] *Scarlet Extended v SABAM*, supra fn. 105, at [44].

This (considerably shortened, due to the focus of the thesis) journey might be commenced at recital 3 of the InfoSoc Directive, which states that the aims of this legal instrument relate to "compliance with the fundamental principles of law and especially of property, including intellectual property, and freedom of expression and the public interest".[941] One could see this as if copyright and the freedom of expression were two sides of the same coin known as "the public interest". On the one hand, copyright was described in the UK copyright case of *Ashdown* as "antithetical to freedom of expression".[942] On the other hand, both sides of this particular pairing might be seen as two different, yet complementary paths to the "development and the diffusion of science and culture", [943] as the ICESCR phrased it.

Helfer and Austin succinctly describe these two competing views on the relationship between copyright and the freedom of expression. The first one is that protecting the former right provides an incentive to express oneself, therefore furthering the interest of the latter concept. The second view is that freedom of expression is restricted by copyright, in the way that the pool of expressible information is limited by the copyrightholders' reach.[944] In this author's view, Akester connects those perspectives in a most convincing manner, when she writes that "at a conceptual level, the rights that underpin access to information and copyright protection are linked within a perpetual cycle of discovery, enlightenment and creation".[945] However, "in spite of this theoretical harmony, those values can challenge each other at a practical level".[946] And, as the following subsections are going to demonstrate, copyright definitely does so in the area of online enforcement, together with the other three interests backing up the enforcement schemes presented in chapter two.

---

[941] Information Society Directive, supra fn. 8, rec. 3.
[942] [2001] EWCA Civ 1142, at [30].
[943] ICESCR, supra fn. 859, art. 15(2).
[944] Helfer and Austin, supra fn. 881, at 222.
[945] Akester P, 'The new challenges of striking the right balance between copyright protection and access to knowledge, information and culture' (2010) E.I.P.R. 32(8), at 372.
[946] Akester, supra fn. 945, at 372.

3.2.1. Removal of access to legitimate content.

The first major conflict area in this section arises from the risk of legitimate content being removed or made inaccessible as a result of the enforcement schemes' operation. Access to legitimate information is protected by the freedom of expression (as it is phrased in art. 11 of the Charter) and hence, it is necessary to consider the enforcement schemes' impact on such access.

The first enforcement measure which carries the risk of limiting access to legitimate content is the notice and takedown regime; and there are two interlinked reasons for this *status quo*. Firstly, the rightholders might send – accidentally or maliciously - their notices for content which is in fact undoubtedly[947] legitimate.[948] This is particularly likely when automated notice sending mechanisms are in use, as Urban et al indicate – in their study, both rightholders and ISPs admitted this to be the case.[949] Secondly, the expected safeguard in the form of the proper assessment conducted by the intermediaries receiving the notice might be less effective than one could imagine it to be. What James wrote in 2012 in the context of defamation holds true for all four content types; the "expeditious removal" requirement of art. 14 of the E-Commerce Directive[950] might be inadvertently putting free speech at risk, for in order to avoid liability and stay within the term "expeditious", (hosting) intermediaries might be inclined to quickly remove access to the content complained of, without due examination.[951] This risk was found to be a current, confirmed one by Urban et al as well, in the context of copyright.[952] The situation is particularly problematic given that the ambiguous term "expeditious" might be interpreted to mean as little as, for example, twenty-

[947] With regards to the not uncommon situations where this is difficult to ascertain (for example, copyright exceptions etc.) please see further paragraphs of the current section.
[948] See, for example, the data on the inaccurate notice and takedown requests received by Google Search, available at https://torrentfreak.com/google-discarded-21000000-takedown-requests-in-2013-131227/
[949] Urban et al, supra fn. 458, at 2.
[950] E-Commerce Directive, supra fn. 91.
[951] James S, 'Tightening the net: defamation reform and ISPs' (2012) Ent. L. R. 23(7), at 197.
[952] Urban et al, supra fn. 458, at 39.

four hours. James accurately remarked that moderating content might be a "relatively high-risk, expensive and labour-intensive"[953] approach, and while this does not make the "remove content as notices come" attitude commendable, it makes it understandable, and together with it, the threat to freedom of expression, for all four content areas.

The variant of notice and takedown warranted in the *Costeja*[954] case deserves to be dealt with in a separate section here. As Hornle noted in her article, the CJEU did not even refer to art. 11 of the CFREU; and it is reflected in its reasoning.[955] As the Advocate General noted in his opinion on the case, whenever someone types in the name of another person into a search engine, he is "actively using his right to receive information concerning the data subject from public sources".[956] This right "would be compromised if his search for information concerning an individual did not generate search results providing a truthful reflection of the relevant web pages". This is especially convincing when the material posted on those websites is legitimate, like in Mr. Costeja's case. The CJEU did not follow the AG's line of reasoning; as Lynskey notes, the Court "did not acknowledge that the removal of data from a search engine rather than a web page also has more significant freedom of expression implications for the very same reasons: it prevents easy access to data for a larger number of individuals".[957] Consequently, the freedom of expression can be seen as severely impaired by the *Costeja*'s notice and takedown procedure.

The second enforcement scheme which deserves similar attention is the one based on content filtering. In contrast to notice and takedown, the threat to freedom of expression posed by such filters is based more on

[953] James, supra fn. 951, at 197.
[954] *Costeja*, supra fn. 196.
[955] Hornle J, 'Google's algorithms, search results and relevancy under data protection law - whose data quality?' (2014) Ent. L. R. 25(6), at 211.
[956] Opinion of the Advocate General delivered on 25 June 2013 in the Case C-131/12, at [130].
[957] Lynskey, supra fn. 867, at 531.

technical/technological concerns (such as overblocking and/or incorrectly oriented filters), rather than on purely human errors or motivations. While this is an issue pertaining to all four content types, the CJEU case law discussing it comes from the area of copyright; hence, the decisions in *Scarlet* and *Netlog* appear again in this chapter.

The filtering procedure requested in the first of the two cases was seen as a measure which "could potentially undermine freedom of information since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications".[958] As it might be remembered, the CJEU in *Scarlet* based its analysis on the balancing exercise between various human rights; the described threat to freedom of expression was one of the three components of this exercise which led to the dismissal of the filtering system sought by SABAM. Similar reasoning was present in the *Netlog* case, where the danger of endorsing a filtering system which is not precise enough in making a distinction between legitimate and infringing content (a danger phrased out by reference to *Scarlet*) also played a part in the Court's dismissal of the filtering system,[959] despite the newer case dealing with a social media website, as opposed to an ISP.

It has to be added that the cited decisions leave certain difficult questions regarding the more precise characteristics of the acceptable (in terms of the freedom of expression) filtering schemes. For example, the CJEU in *Scarlet* dismissed "an injunction made against an internet service provider which requires it to install a system for filtering all electronic communications passing via its services, in particular those involving the use of peer-to-peer software, which applies indiscriminately to all its customers, as a preventive measure, exclusively at its expense; and for an unlimited period".[960] Does this mean that the designers of filtering systems should avoid implementing the

[958] *Scarlet Extended v SABAM*, supra fn. 105, at [52].
[959] *SABAM v Netlog*, supra fn. 103, at [50].
[960] *Scarlet Extended v SABAM*, supra fn. 105, at [29].

cited combination of elements, or each one of them independently? Moreover, does each of those elements interfere with freedom of expression, or are some of them related to other human rights which were placed by the CJEU against the right to property? According to the Attorney-General's opinion in *Scarlet*, the danger to freedom of expression is inherent in content filtering systems, regardless of their specifics.[961] Nevertheless, it is worth searching for solutions mitigating this threat, and hence, the conclusive chapter of this thesis provides a contribution to the search for the best possible filtering system in terms of its "freedom of expression footprint".[962]

The third example of an enforcement scheme the operation of which might impair access to legitimate content is that of the criminal law-based shutdowns of online services. For example, whenever a website hosting a considerable amount of infringing content is shut down (its operators arrested, its servers seized), there is a possibility that a certain amount of non-infringing content is going to be made unavailable to its legitimate owners. This occurred, for example, after the Megaupload shutdown, when Leaseweb (Megaupload's hosting provider) deleted the cyberlocker users' data from its servers without prior warning.[963] While one could argue that users should have retained offline copies of the files they lost access to, this does not change the fact that an infringement with their right set out in art. 11 of the CFREU took place. Another, slightly more contentious example would be the shutting down of a pornographic website on which a significant amount of revenge pornography is hosted; one could argue that users who shared their own, non-infringing videos on that website had their freedom of expression encroached upon: though extending the human right in question to "the right to expose oneself in cyberspace" would be a challenging (yet an interesting) endeavour.

[961] Opinion of AG Cruz Villalón in *Scarlet Extended*, supra fn. 539, at [86].
[962] See section 2.3.1.2 of chapter five.
[963] See https://torrentfreak.com/leaseweb-wipes-all-megaupload-user-data-dotcom-outraged-130619/

Website blocking injunctions also have the potential to remove access to legitimate content, much in the same manner as the criminal law shutdowns. As for the risks particular to the former, the discussed concern might arise when in order to remove a branch, a whole tree is cut down: when only, for example, a separable section of a website is hosting infringing content, but the whole domain becomes blocked – a concern also raised by Angelopoulos.[964]

The DRM systems (hereafter referred to as the DRMs) provide a final example in this section. Being based on the limitation of what a user can do with a piece of content, they continuously operate near the edge of interference with the users' freedom of access to information. While not directly aimed at the cyberspace setting, a study conducted by Akester in 2010[965] explored the relationship between DRMs and the human right in question by looking at whether this enforcement scheme prevents "librarians, visually impaired, private users, lecturers, students and researchers from performing actions they are allowed to perform".[966] She concluded that DRMs did not have a massive impact on the acts permitted by law, but they did have some adverse effect. Moreover, technological solutions implemented in order to allow space for legitimate acts did not, overall, perform sufficiently well.[967]

The examples presented in the previous paragraphs portrayed the threat posed by the enforcement schemes to legitimate content existing in cyberspace. However, as it was mentioned in the introduction to chapter one, the concept of infringing content is at times, a slightly artificial one; for example, it is not fully certain whether a video on a streaming website is covered by a copyright exception unless the court confirms that this is the case. While this thesis is focused on the removal of access to infringing content, and on finding the most adequate way of doing this, it cannot be omitted that many enforcement schemes (for example, notice and takedown, website blocking injunctions,

[964] Angelopoulos, supra fn. 933, at 815.
[965] Akester P, 'The impact of digital rights management on freedom of expression - the first empirical assessment' (2010) IIC 41(1), at 31.
[966] Akester, supra fn. 965, at 36.
[967] Akester, supra fn. 965, at 38.

criminal law-based shutdowns) pose a freedom of expression-related threat not only to legitimate content of "untarnished" character, but also to digital content which *might be* infringing, depending on whether it is covered by relevant exceptions, such as fair dealing (a copyright example),[968] or the overwhelming public interest in having the infringing work made widely accessible (a fitting example for the areas of privacy and defamation).

A quote from *Scarlet* supports this line of concern: "(i)ndeed, it is not contested that the reply to the question whether a transmission is lawful also depends on the application of statutory exceptions to copyright which vary from one Member State to another. Moreover, in some Member States certain works fall within the public domain or can be posted online free of charge by the authors concerned".[969] This notion was also repeated later on in *Netlog*[970] and Ponte remarked upon it when writing about the US measures aimed at movie piracy: "First Amendment advocates are concerned that the further criminalization of copyright violations places a chilling effect on free speech and continues to *dismantle fair use principles* in this march toward zero tolerance against movie copyright violations".[971]

Taking defamatory content as another example; defences to the tort of defamation (as it was described in section 5.1 of chapter one) can also turn an *a priori* infringing piece of content into a legitimate one, the removal of access to which would go against freedom of expression. In the UK law, three primary defences of this kind can be distinguished; justification, fair comment and privilege (absolute or qualified). All three were updated in recent years by the Defamation Act 2013, and all three are laid out in the following paragraphs.

---

[968] See, for example, section 30 of the CDPA 1998 c. 48.
[969] *Scarlet Extended v SABAM*, supra fn. 105, at [52].
[970] *SABAM v Netlog*, supra fn. 103, at [50].
[971] Ponte L, 'Coming Attractions: Opportunities and Challenges in Thwarting Global Movie Piracy' (2008) 45 AM. BUS. L.J. 331, at 335, emphasis added.

In principle, the defence of justification rested on the premise that the allegedly defamatory statement is, in fact, true. The underlying idea behind it was that one should not be entitled to be compensated for a reputation that he does not deserve, as it was stated in the case of *McPherson v Daniels* (1829).[972] Given the high value placed by the English law on one's reputation, it is potentially predictable that the burden of proof rested here on the defendant[973] – he had to prove that the statement in question is true. However, after many years of service, the common law defence of justification was abolished by section 2 of the Defamation Act 2013 and replaced with the so-called "truth" defence.[974] It retains the core reasoning of its predecessor,[975] while updating the earlier defence in two key aspects; firstly, it specifies (following the case of *Chase v News Group Newspapers Ltd* (2002)[976]) that even if a part of the contested statement is not true, as long as its substantial component (one which carries the actual defamatory meaning) is found to be true, the defence still applies.[977] Secondly, the truth defence allows for the recognition of multiple imputations of the statement in question; it is still possible to qualify for it if the non-defamatory imputations are not proven to be true.[978]

The second defence traditionally present in the English law of defamation was that of fair comment or, as Lord Phillips renamed it in the case of *Joseph v Spiller* (2010),[979] honest comment. It applied to situations where the statement in question was recognised to constitute an opinion,[980] based on a sufficient

[972] 10 B. & C. 263, at 272.
[973] Price D and others, *Defamation: Law, Procedure and Practice* (Sweet and Maxwell 2010), at 59.
[974] What matches the suggestion made in the *Report of the Faulks Committee on Defamation* (Cmnd 5909) (1975), at [5a].
[975] Defamation Act 2013, supra fn. 212, s. 2(1) – "It is a defence to an action for defamation for the defendant to show that the imputation conveyed by the statement complained of is substantially true".
[976] [2002] EWCA Civ 1772.
[977] Defamation Act 2013, supra fn. 212, s. 2(3).
[978] Defamation Act 2013, supra fn. 212, s. 2(2).
[979] [2010] UKSC 53 at [117].
[980] For consideration of what constitutes an opinion, see, for example, *Hunt v Star Newspaper Co Ltd* [1908] 2 KB 309 at 319, *Telnikoff v Matusevitch* [1992] 2 AC 343, and *Galloway v Telegraph Group Ltd* [2006] EWCA Civ 17.

factual basis,[981] and made in relation to a matter of public interest (defined broadly by Lord Denning MR in *London Artists v Littler* (1969), who declared that "whenever a matter is such as to affect people at large, so that they may be legitimately interested in, or concerned at, what is going on; or what may happen to them or to others; then it is a matter of public interest on which everyone is entitled to make fair comment"[982]). Similarly to justification, this defence was also abolished and given new form by the Defamation Act 2013. It evolved into the "honest opinion" defence, which no longer requires the opinion to be made on the matter of public interest. It is sufficient if the statement was an opinion, indicated its factual basis, and an honest person could have held the expressed opinion on such basis.[983]

The third key defence of English defamation law is that of absolute or qualified privilege. It rests on the idea that in certain situations, where the claimant's reputation was indeed damaged by the contested statement, the defendant should nevertheless be protected from liability in the interest of free speech and freedom of expression.[984] Absolute privilege provides absolute protection from liability, but has a very narrow scope – it applies to instances such as judicial and parliamentary proceedings.[985] Qualified privilege provides a defence which, in contrast, is not absolute and might be defeated – if it is proven that the statement was published with malice. The qualified privilege defence can be found "where the person who makes a communication has an interest, or a duty, legal, social or moral, to make it to the person to whom it is made, and the person to whom it is made has a corresponding interest or duty to receive it".[986] For the purposes of this thesis, out of various scenarios which were recognised to fulfil this test, it is worth discussing one particular mode of qualified privilege known as the *Reynolds* defence, established in the House of

[981] For example, see *Merivale v Carson* (1887) 20 Q.B.D. 275, *Kemsley v Foot* [1952] A.C. 345, and *Lowe v Associated Newspapers Ltd* [2006] EWHC 320 (QB).
[982] [1969] 2 Q.B. 375, at 391.
[983] Defamation Act 2013, supra fn. 212, s. 3.
[984] As well as, one could add, maintaining the legal and political processes efficient, or even viable.
[985] See, for example, *Trapp v Mackie* [1979] 1 W.L.R. 377.
[986] *Adam v Ward* [1917] A.C. 309, at 334.

Lords case of *Reynolds v Times Newspapers Ltd* (1999).[987] It expanded qualified privilege to cases where the media report on matters of public interest by means of published statements which ultimately turn out to be false (and defamatory), despite their authors having taken reasonable steps when obtaining the factual basis of the statement. A characteristic scenario of this kind would be a situation where a journalist receives a false piece information from his confidential source, concerning the conduct of, for example, a politician or a judge.

While the defence of qualified privilege *per se* is still available at the time of writing, the *Reynolds* defence was abolished and replaced by s. 4 of the Defamation Act 2013, which created the defence of "publication on matter of public interest". The core element of the latter, set out in s. 4(1) of the Act, is that it "it is a defence to an action for defamation for the defendant to show that the statement complained of was, or formed part of, a statement on a matter of public interest; and the defendant reasonably believed that publishing the statement complained of was in the public interest".[988] Further subsections of s. 4 purport to clarify certain doubts which were tied to the *Reynolds* defence, such as when is it reasonable for the defendant to believe that his actions are in the public interest[989] or whether the statement in question can be an opinion.[990] Additionally, it is fairly clear that the new defence is available not only to major commercial publishers, such as The Times newspaper, but to anyone who publishes statements in the manner described above. In the age of Facebook, Twitter, WikiLeaks, as well as countless blogs and forums, this defence could apply to a multitude of scenarios concerned with defamatory content in cyberspace.

It has to be noted that in the online setting, those defences are relied on very rarely, if at all – not many people are willing to, for example, defend their blog

[987] [1999] 3 W.L.R. 1010.
[988] Defamation Act 2013, supra fn. 212, s. 4(1).
[989] Defamation Act 2013, supra fn. 212, s. 4(3).
[990] Defamation Act 2013, supra fn. 212, s. 4(5).

posts or Usenet postings in court, due to the rather understandable lack of time and money, as it was rightly pointed out by McEvedy.[991] However, even if none of the three defences described above applies, a claim aimed at legal recognition of specific online content as defamatory (and subject for removal) might fail if the court decides that granting the claimant his wish would constitute an abuse of the process of the court. One of the premises which could lead to such a decision is the failure to satisfy the "real and substantial tort" requirement. In the context of defamation law, such a failure might occur when the protection of claimant's reputation is not the primary aim of the claim, or when the cost of pursuing the claim would be out of all proportion to the benefit.[992] Additionally, allegedly defamatory statements made online might often turn out to be mere vulgar abuse, not causing actual, actionable damage to reputation: as was mentioned in the case of *Smith v ADVFN* (2008).[993]

Finally, there is a further dimension of the threat posed to legitimate (or potentially legitimate) content by the enforcement schemes, materialising whenever the intermediaries are asked to assess the legitimacy of content complained of. It is questionable whether the technology companies are the right party (in terms of expertise and democratic mandate) to decide on whether, for example, there is a sufficient public interest in preserving access to a piece of infringing content (a situation triggered by, for example, the approach endorsed in the *Costeja* case.[994]) Desirable protection of freedom of expression in this area demands that the best possible party takes the decision on whether factors such as exceptions to infringement materialise in a piece of content. Certainly, both content owners and users have the option of challenging the intermediary's decision in court: however, what was true in the previous paragraph for allegedly defamatory content is likely to be true for the other content types as well: few have the time and money to protect their

[991] McEvedy L, 'Defamation and intermediaries: ISP defences' (2013) C.T.L.R. 2013, 19(4), at 108.
[992] *Jameel v Dow Jones*, supra fn. 216, at [71].
[993] *Smith v ADVFN*, supra fn. 213, at [24].
[994] *Costeja*, supra fn. 196.

freedom of expression in such a scenario, and potential harm done might be difficult to rectify.

3.2.2. Removal of access to infrastructure which could be used for sharing legitimate content.

A fair amount of enforcement schemes includes rendering an online service unavailable; while this might prevent a considerable amount of infringing activities, the loss of access to the service in question might impair the online society's ability to express and receive legitimate information. Additionally, the operator of the service himself might be perceiving his inability to facilitate the exchange of legitimate content as an infringement of the right guaranteed by art. 11 of the Charter. The following paragraphs are going to discuss both aspects of the problem, consecutively.

The first example of an enforcement scheme which creates a risk of interference with the online public's freedom of expression in the described manner is the notice and takedown regime aimed at indexing services. To provide specific situations demonstrating this concern: it might occur whenever a metasearch engine such as Filestube is asked to delist a specific cyberlocker from its service, or whenever a search engine such as Google is asked to delist all results from a specific auction website or from a blogging platform.

Another fitting example would be the use of ISP-oriented blocking injunctions. The CJEU copyright case of *UPC Telekabel* (2014)[995] not only provides a supporting factual scenario, but also contains the discussion of the arising interplay between the human rights involved. In the initial proceedings, the claimant ISP challenged an injunction obliging it to block access to a

[995] Case C-314/12 *UPC Telekabel v Constantin Film* (2014).

website on which the defendant's movies were made available without the latter's consent. More specifically, the injunction asked UPC Telekabel "to block the access of its customers to the website at issue".[996] The CJEU, inquired about the validity of such an injunction, based its response on the premise that, in the current scenario, a balancing exercise has to be conducted between the rightholder's right to property, the ISP's freedom to conduct a business (on which see more in section 3.3 of the current chapter) and the *users' freedom of expression*.[997] The requested injunction was seen to be compatible with the EU law, provided that (inter alia) the ISP relies on measures which respect its users' freedom of expression and "do not unnecessarily deprive internet users of the possibility of lawfully accessing the information available".[998] Given the wording of art. 11 of the CFREU, it could be also assumed that the described condition also covers the possibility of *expressing* lawful information.

This is one of those points where the CJEU's answer gives rise to plenty of further questions. Removal of access to any website or platform deprives the users of the described possibilities; what should be the guiding notion in the search for "unnecessary" deprival? The presence/availability of alternative platforms? How many of them should exist? What if the blocked website offers more sophisticated and/or more comfortable ways of exchanging lawful information than the alternatives?

It is also worth bringing the attention to another case which examined the impact of the ISP blocking injunctions on the users' freedom of expression; namely, *EMI Records v British Sky Broadcasting*.[999] In this UK decision, Arnold J regarded the right to property standing behind the requested blocking injunction as "clearly outweighing the Charter article 11 rights of the users of

[996] *UPC Telekabel*, supra fn. 995, at [11].
[997] *UPC Telekabel*, supra fn. 995, at [47].
[998] *UPC Telekabel*, supra fn. 995, at [63]. It is worth to note that "accessing information available" might be indicating both the information which is already in cyberspace, as well as information which might appear there in the future.
[999] *EMI v Sky*, supra fn. 119.

the websites, who can obtain the copyright works from many lawful sources".[1000] Without denying the logic behind this line of reasoning, the judgment in *EMI* fails to take account of the possibility of lawful content appearing (or already existing) on the blocked website; and this is most likely to be true for other *Newzbin* injunction cases.[1001] The questions which appeared in relation to the *UPC* case remain here as well.

There is an additional, specific dimension of the discussed type of interference with the online public's freedom of expression, tied to IP address–based website blocking. There is a possibility that an IP address attached to the targeted "illicit" website is shared with an unrelated legitimate website. Should the former's IP address become blocked, the latter might be caught in the crossfire. This concern was raised in the *Dramatico (No. 2)* case, where Arnold J stated that "IP address blocking is generally only appropriate where the relevant website's IP address is not shared with anyone else. If it is shared, the result is likely to be overblocking".[1002] As The Pirate Bay's address was viewed as not being shared with anyone else, this line of concern did not prevent the blocking injunction from being granted – but it is a problem which has to be kept by the policymakers in mind.

Technological measures of the graduated response schemes,[1003] impairing the quality of or disabling the user's Internet connection altogether, can also be seen as an enforcement scheme threatening the users' freedom of expression through the removal of infrastructure which could be used for the exchange of legitimate content. Akester's article from 2010 brings support to this position when it states that "(t)he possible sanction of suspension of the internet accounts of repeat copyright infringers may affect human rights - where internet access is seen as an instrument for promoting the realization of the human rights as defined in arts 19 and 27 of the Universal Declaration of

[1000] *EMI v Sky*, supra fn. 119, at [107].
[1001] Covered in section 3.1.2.3.1 of chapter two.
[1002] *Dramatico (No. 2)*, supra fn. 117, at [13]
[1003] Covered in section 2.4 of chapter two.

Human Rights".[1004] Discussion of Hert and Kloza's analysis set out in section 2.3 of the current chapter can be referred to in a similar manner.[1005]

For the final example, website shutdowns based on criminal law - such as those described in section 3.2 of chapter two – are also removing access to online intermediaries, and hence can be seen as a similar threat to the users' freedom of expression.

As it was mentioned, an online intermediary whose service had access to it removed or impaired through one of the enforcement schemes can also be seen as having its freedom of expression infringed upon. This could be dubbed as "the right to be a facilitator of communications" and it received a considerable amount of attention in two ECtHR cases: *Neij and Sunde Kolmisoppi v Sweden*[1006] (copyright-based) and *Delfi AS v Estonia*[1007] (defamation-based). Those decisions are analysed in the following paragraphs.

The factual background of the *Neij* case centred on The Pirate Bay (hereafter referred to as TPB) operators' attempt to overturn their convictions from 2009 (discussed above[1008]), on the basis of the alleged infringement of art. 10 of the ECHR. The Court stated that "the applicants put in place the means for others to impart and receive information" and proclaimed that such an activity merits the protection of art. 10(1) of the Convention.[1009] However, the judges went on to stress that according to art. 10(2), freedom of expression has to be balanced against a set of other legitimate interests;[1010] among them, the right to property, which was infringed on TPB multiple times. It was decided that the interference with the claimant's freedom of expression could be seen as prescribed by law, following a qualified legitimate interest and necessary in a

[1004] Akester, supra fn. 945, at 380.
[1005] Hert and Kloza, supra fn. 851.
[1006] *Neij v Sweden*, supra fn. 891.
[1007] *Delfi AS v Estonia*, supra fn. 873.
[1008] See section 2.2.3.1 of chapter one.
[1009] *Neij v Sweden*, supra fn. 891, at 9.
[1010] *Neij v Sweden*, supra fn. 891, at 10.

democratic society.[1011] The fact that the operators of TPB did not take any action aimed at removing the torrent files complained of was seen as an important factor in the latter finding.[1012]

This is a very significant decision: as Jones noted, the ECtHR recognised a new manner of exercising one's freedom of expression, which deserves protection regardless of being tied to (copyright-) infringing content.[1013] However, Jones also expressed concern that the wide margin of interpretation left for the signatories' courts might constrain the development of the "freedom of expression" defence for the intermediaries.[1014] Tracking the ripple effect of the decision in *Neij* is certainly a worthy endeavour in this area of research; while a blanket, untouchable defence of the "freedom of expression's facilitator" would be ill-advised, further recognition of this aspect of the right set out in art. 11 of the Charter would be a welcome analytical shift.

The second ECtHR case in which the right to being a facilitator of other's communications was discussed is the case of *Delfi AS*. Here, the applicant was an operator of a news portal with comment-making facilities. L, owner of a company which was accused in an article posted on Delfi of destroying an ice road, was subjected to multiple defamatory and offensive comments posted under the article in question. The website's operators removed the said comments on the same day as L notified them about the infringing content. Nevertheless, L claimed the equivalent of 32,000 euros in damages, and the case went into the Estonian courts.[1015] After the Tallinn's Court of Appeal ruled in favour of L and stated that Delfi should have exercised preliminary control over comments posted on its portal, the latter filed an application to the ECtHR.

[1011] *Neij v Sweden*, supra fn. 891, at 11.
[1012] *Neij v Sweden*, supra fn. 891, at 11.
[1013] Jones J, 'Internet pirates walk the plank with article 10 kept at bay: Neij and Sunde Kolmisoppi v Sweden' (2013) E.I.P.R. 35(11), at 697.
[1014] Jones, supra fn. 1013, at 697.
[1015] *Delfi AS v Estonia*, supra fn. 873, at [14].

Now, this is a slightly different scenario than that in *Neij*; here, the intermediary is still allowed to be a facilitator of online communications. Nevertheless, the discussed infringement of freedom of expression could still be seen as having occurred, as the applicant's facilitating activity can be seen as impaired by the requirement of preventive monitoring. Consequently, Delfi complained that making it liable for the comments was an infringement of its rights under art. 10 of the ECHR, that "the obligation imposed on it to maintain a preventive censorship policy over the exercise of freedom of expression of third persons also infringed its freedom of expression, that is freedom to impart information created and published by third persons".[1016] This submission was accepted by the Court – however, the interference with Delfi's freedom of expression was found to be prescribed by law, necessary in democratic society and supported by one of the legitimate interests set out in art.10(2): in this case, the right to privacy, covering the injury to reputation.[1017]

In balancing the two human rights facing each other in the present *Delfi* case, the ECtHR placed more weight on L's reputation than on Delfi's freedom of expression, accepting the approach of the Estonian courts. Factors which, among others, informed this decision were: that since the contested article carried a significant risk of attracting offensive/defamatory comments and the number of comments was above the average, Delfi should have exercised "a degree of caution in the circumstances of the present case in order to avoid being held liable for an infringement of other persons' reputations";[1018] that the keyword filter (implemented by Delfi) was insufficient in itself for preventing harm being caused to third persons;[1019] and that the applicant "was in a position to know about an article to be published, to predict the nature of the possible comments prompted by it and, above all, to take technical or manual measures to prevent defamatory statements from being made

[1016] *Delfi AS v Estonia*, supra fn. 873, at [49].
[1017] *Delfi AS v Estonia*, supra fn. 873, at [94].
[1018] *Delfi AS v Estonia*, supra fn. 873, at [86].
[1019] *Delfi AS v Estonia*, supra fn. 873, at [87], this finding seems to be in accordance with the analysis conducted in section 2.3 of chapter three.

public".[1020] Moreover, requesting the claimant to go after the comments' authors was regarded by the Court as too difficult and burdensome for him, as it would be an approach not guaranteeing the adequate protection of art. 8. Ultimately, Delfi was also ordered to pay three hundred and twenty euros to L.[1021] The referral of this case to the Grand Chamber of the ECtHR, which gave its judgment in June 2015,[1022] largely confirmed the analysed First Section's judgment.

What can be inferred from this decision is that the ECtHR does not regard preventive monitoring practices as a disproportionate interference with the online intermediaries' freedom of expression. Furthermore, considering the factors which supported the Court's decision, it is difficult to envisage conditions under which the intermediaries' freedom of expression would outweigh the rightholders' interests in the discussed type of a scenario, unless the infringement of such interests was to be minimal.

3.3. The four protected interests vs the freedom to conduct a business.

3.3.1. Imposing duties on intermediaries as an infringement of the freedom to conduct a business.

As it has to be clear by this point, a common characteristic of many enforcement schemes is that they place certain obligations on the online intermediaries connected to the transfer of infringing content. Such obligations might be burdensome to a lesser or greater extent, this ranging from a nigh unnoticeable burden to a challenge to the online service's business model.

[1020] *Delfi AS v Estonia*, supra fn. 873, at [89]. This stance can be contrasted with the E-Commerce Directive's regime, explored in section 3.3 of chapter two.
[1021] *Delfi AS v Estonia*, supra fn. 873, at [93].
[1022] The Grand Chamber ruling in *Delfi AS v Estonia* (2015), application no. 64569/09.

Regardless of where they stand on this scale, such obligations may be regarded as interfering with the online intermediaries' freedom to conduct a business, protected by art. 16 of the CFREU. They are not the ones who decided to share infringing content and yet they are asked to take steps for the benefit of the rightholders, their standard business activity being disturbed.

The first enforcement scheme to be discussed in this section is the notice and takedown procedure. Processing notices takes time and resources, as well as requires trained personnel to assess their validity. In Urban et al's study, the interviewed ISSPs "described discomfort with both the cost and the substantive judgment associated with assessing the accuracy of takedown requests".[1023] Within the EU, the "expeditious removal" requirement of art. 14(1) of the ECD might be seen as placing additional pressure and an additional burden on the intermediaries, which might turn out to be even greater (or even oppressive, as Edwards put it[1024]) due to the fact that the term "expeditious" might indicate periods of time as short as twenty-four hours, depending on the courts' interpretation.

Secondly, preventive monitoring obligations might be quite a burden as well, whether we consider the more "manual" supervision of content (about which James wrote that it might be a "relatively high-risk, expensive and labour-intensive" approach[1025]), or the more "technological" aspect of this approach, represented by the content filtering schemes.[1026] In its endeavour to discuss the latter in more depth, this section refers to two CJEU cases – *Scarlet Extended* and *Netlog*. In the former, the contested injunction was seen by the Court as placing a significant burden on the defendant ISP, by requiring it to install a filtering system which monitors *all* the electronic communications made on its network.[1027] Furthermore, this obligation was not limited in time, was directed at all future infringements and was "intended to protect not only existing

[1023] Urban et al, supra fn. 458, at 35.
[1024] Edwards, supra fn. 594, at 10.
[1025] James, supra fn. 951, at 197.
[1026] Such as those described in section 3.1.2.2 of chapter two.
[1027] *Scarlet Extended v SABAM*, supra fn. 105, at [47], emphasis added.

works, but also future works that have not yet been created at the time when the system is introduced".[1028] Gathering those factors together, the CJEU stated that "such an injunction would result in a serious infringement of the freedom of the ISP concerned to conduct its business since it would require that ISP to install a complicated, costly, permanent computer system at its own expense". This was backed by a reference to art. 3 of the Enforcement Directive, which requires the IP enforcement measures to avoid being "unnecessarily complicated or costly".[1029] Consequently, the filtering scheme was regarded as not striking the adequate balance between the right to property and the freedom to conduct a business, for it was putting the latter at an excessive risk.[1030]

Moving on to the *Netlog* case. As it might be remembered, the filtering scheme requested in those proceedings entailed filtering all users' information indiscriminately, as a preventative measure, exclusively at the social network provider's expense and for an unlimited period of time.[1031] The CJEU stated that accepting such a filtering system would "result in a serious infringement of the freedom of the hosting service provider to conduct its business since it would require that hosting service provider to install a complicated, costly, permanent computer system at its own expense (…)".[1032] Similarly to the filter in *Scarlet*, this one was also regarded as not striking the adequate balance between the protection of IP rights and the freedom to conduct a business.[1033]

While those judgments do not provide us with direct guidance on how to devise a preventive filtering system which is not overly oppressive on the right set out in art. 16 of the CFREU, the factors they refer to might be of some help in this task, not only in the context of injunctions aimed at ISPs or social

[1028] *Scarlet Extended v SABAM*, supra fn. 105, at [47].
[1029] *Scarlet Extended v SABAM*, supra fn. 105, at [48].
[1030] *Scarlet Extended v SABAM*, supra fn. 105, at [49]. It is worth adding that the Attorney General sought to rely on the right to property in order to protect the intermediaries in such scenarios, Supra fn. 539, at [71].
[1031] *SABAM v Netlog*, supra fn. 103, at [26].
[1032] *SABAM v Netlog*, supra fn. 103, at [46].
[1033] *SABAM v Netlog*, supra fn. 103, at [47].

networks, but also those aimed at other online intermediaries, and those coming from other content type areas.

The ISP-aimed blocking injunctions provide for another arena on which the human rights-backed enforcement schemes might interfere with the freedom to conduct a business. Here, the earlier mentioned CJEU case of *UPC Telekabel*[1034] might be relied on as the key useful point of reference. As it might be remembered from section 3.2.2 of this chapter, the CJEU stated that in order to assess the validity of the contested blocking order, a balancing exercise has to take place: with the rightholders' right to property on the one hand, and the users' freedom of expression plus the intermediaries' freedom to conduct a business on the other hand. This time let us look towards the parts of the judgment focused on the latter human right.

Firstly, the CJEU noted that the injunction at hand forces the ISP to "take measures which may represent a significant cost for him, have a considerable impact on the organisation of his activities or require difficult and complex technical solutions".[1035] However, the judges continued by stating that the "injunction does not seem to infringe the very substance of the freedom of an internet service provider such as that at issue in the main proceedings to conduct a business".[1036] This finding was supported by two factors; the first one being that the ISP has a choice of technical measures needed to fulfil the conditions of the injunction,[1037] with the second one based on the premise that, should Telekabel be able to prove that they took all reasonable measures, they would not be liable to the rightholders.[1038] Concluding, the Court found the requested type of an injunction to be compatible with EU law, provided that it allows the ISP for the choice of measures, includes the I-did-all-I-reasonably-could safeguard and the measures employed "do not unnecessarily deprive internet users of the possibility of lawfully accessing the information

[1034] *UPC Telekabel*, supra fn. 995.
[1035] *UPC Telekabel*, supra fn. 995, at [50].
[1036] *UPC Telekabel*, supra fn. 995, at [51].
[1037] *UPC Telekabel*, supra fn. 995, at [52].
[1038] *UPC Telekabel*, supra fn. 995, at [53].

available"[1039] and are effective enough, that is to say that they prevent access to infringing content (or at least make it difficult to obtain such access) and deter users from accessing such content.[1040]

This judgment raises certain difficult questions concerning the actual impact of the freedom to conduct a business's role as a counterweight to the blocking injunction request and enforcement schemes in general. Firstly, the I-did-all-I-reasonably-could safety valve is a rather uncertain one; how should one decide whether the ISP took *all reasonable measures*? The answer provided to this question might lead to a very significant impairment of the ISP's freedom to conduct a business, caused by – as James put it - a "considerable economic and administrative impact on the business models of ISPs".[1041] Furthermore, it seems that this case suggests that the freedom to conduct a business could override the right to property supporting the injunction only if the interference with the former would be threatening the very foundation of the online service in question; which could be regarded as an overly narrow approach.

This notion is remarked upon by O'Sullivan, who stated that the CJEU's invocation of art. 16 of the Charter as a counterweight in *UPC* was largely artificial and, moreover, that art. 12(3) of the E-Commerce Directive[1042] can be seen as a gateway to the reduction in freedom to conduct a business' reach in this area of law.[1043] Husovec adds to this critique by indicating an additional problem tied to placing the debate on what constitutes inappropriate interference (with the right protected by art. 16) within the enforcement proceedings (ie. following the grant of an injunction), as opposed to the main proceedings (preceding the grant of an injunction). The former scenario, furthered by the Court's decision, lays the burden of proof on the intermediary, a burden which joins the pressure to obey the open-ended

[1039] *UPC Telekabel*, supra fn. 995, at [63].
[1040] *UPC Telekabel*, supra fn. 995, at [63].
[1041] James S, 'Digesting Lush v Amazon and UPC Telekabel: are we asking too much of online intermediaries?' (2014) Ent. L.R. 2014, 25(5), at 177.
[1042] Described in section 3.3.1 of chapter two.
[1043] O'Sullivan, supra fn. 712, at 581.

blocking injunction in a timely manner.[1044] It should be added that such pressure (encroaching on the freedom to conduct a business) can also lead to intermediaries adopting measures which might impair the human rights of their users (such as privacy or freedom of expression) for the sake of effectiveness – elaborating on this risk, Husovec indicates the use of deep packet inspection as a potential example,[1045] and James notes that following the *UPC* decision, an ISP might face "liability towards its own customers if any measures it takes (e.g. blocking access to websites) infringe the customers' fundamental rights by impairing their rights to lawfully access information".[1046]

The Hague Court of Appeal's decision in a similar case[1047] (centred on blocking access to The Pirate Bay) provides for an interesting development on the notion of the ISP blocking injunction's effectiveness as a criterion required to overcome the freedom to conduct a business. While the Dutch court found that the number of visits to the torrent website was reduced following the blockade's enactment, it regarded this measure as ineffective, as the users could circumvent it and access the copyright-infringing content from other sources.[1048] Consequently, the block was not deemed to be effective enough to justify the interference with the ISPs' freedom to conduct a business: even though the latter did not challenge the rightholders' assertion that the operative costs of this measure for the ISPs were not overly high.[1049] A somewhat different approach was adopted by Arnold J in the *EMI* case,[1050] where he stated that "a blocking order may be justified even if it only prevents access by a minority of users".[1051]

[1044] Husovec M, 'CJEU allowed website-blocking injunctions with some reservations' (2014) Journal of Intellectual Property Law & Practice, Vol. 9, No. 8, at 632.
[1045] Husovec, supra fn. 1044, at 632.
[1046] James, supra fn. 1041, at 177.
[1047] *Ziggo & XS4ALL v BREIN* (2012) Hague Court of Appeal, case 200105418-01. See http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHDHA:2014:88
[1048] *Ziggo v BREIN*, supra fn. 1047, at [5.1].
[1049] *Ziggo v BREIN*, supra fn. 1047, at [5.22].
[1050] *EMI v Sky*, supra fn. 119.
[1051] *EMI v Sky*, supra fn. 119, at [104].

According to O'Sullivan, the notion of effectiveness should not be a factor in the balancing exercise aimed at deciding whether freedom to conduct a business should nullify the blocking injunction.[1052] He submits that the issue of "effectiveness is a variable that has no role in determining whether or not the Charter should apply to mitigate the scope of those obligations", for the issues of costs and compliance do not arise in the context of blocking injunctions aimed at websites facilitating access to copyright-infringing content.[1053] It is respectfully submitted that this is not a recommendable approach; a measure which is more effective *can* be seen as a stronger (though not necessarily absolute) justification for the interference with the freedom to conduct a business and other relevant human rights (such as the right to privacy and freedom of expression). While the approach adopted in the Dutch TPB case is probably too restrictive in demanding practically impervious measures and giving undue attention to the presence of alternative sources of infringing content, and while regarding the prevention of the minority of users from accessing the website as sufficient could be seen as too broad, the right point of balance (for all enforcement schemes, and all content types) seems to be placed between those two stances.

Another area of conflict relevant for this section of the chapter arises with regards to the identification measures and the costs they bring for the ISPs. While further empirical research aimed at estimating the weight of this burden would be most welcome, some writers brought attention to this concern; for example, Tsoutanis wrote that "(i)n practice, getting ISPs to identify their customers often involves much uncertainty, high cost and significant delays for everybody involved".[1054]

The final conflict area to be considered in this section centres on the costs of running the graduated response schemes. The Digital Economy Act 2010 (covered in section 2.4 of chapter two) can be used here as an example.

[1052] O'Sullivan, supra fn. 712, at 583.
[1053] O'Sullivan, supra fn. 712, at 583.
[1054] Tsoutanis, supra fn. 324, at 954.

Firstly, there are the costs of running the initial obligations procedure; this includes receiving and processing the Copyright Infringement Reports (hereafter referred to as the CIRs), maintaining the records on how many CIRs each of their subscribers attracted, as well as providing the lists of users above the threshold to the rightholders. Furthermore, running the technological measures component of the Act would include the costs of implementing various connection-affecting procedures on the ISPs' subscribers. According to Edwards, imposing the burden resulting from the described obligations on the ISPs would not be just or sensible; nor would it be so to require the entities such as universities, libraries, and Wi-Fi hotspots to monitor the use of their connection for infringements which could attract the CIRs.[1055] By extension, such concerns could be related to the cited intermediaries' freedom to conduct a business.

[1055] Edwards, supra fn. 361, at 537.

Chapter 5 – Towards the "specified request" model of intermediary liability.

1. Introduction.

Having explored various challenges related to the enforcement schemes' effectiveness in chapter three, and having analysed the principal human rights-oriented conflicts present in this area of online regulation in chapter four, this thesis arrives at its fifth and final chapter. Its aim is to put forward a set of recommendations aimed at improving the capability of this branch of EU law to respond adequately to the issues described in the preceding chapters.

There are multiple forms which this chapter could take, multiple aspects of the previous four chapters which it could focus on. Ultimately, instead of trying to produce a long list of independent tweaks this regulatory area could benefit from, the fifth chapter is focused on a single, complex and far-reaching proposition, built around a major upheaval of the approach to intermediary liability in the EU, an upheaval which could provide a worthy response to the wide range of concerns identified in chapters three and four.

This choice is first and foremost justified by the undeniable importance of pinpointing and/or reviewing the ISSPs' place in the online enforcement process, an importance evidenced in the previous chapters of this thesis. Endorsing such an analytical perspective is particularly beneficial in the European context, given the EU legislators' recent initiatives and regulatory objectives, visible in, for example, the Digital Single Market communication. This document (laying out the EU Commission's agenda for the digital environment) states that "(t)he Commission will launch before the end of 2015 a comprehensive assessment of the role of platforms, including in the sharing economy, and of online intermediaries, which will cover issues such as (…)

how best to tackle illegal content on the Internet".[1056] It is hoped that this conclusive chapter is going to provide a valuable contribution to this and further assessments, in 2016 and beyond.

2. Specified request vs blunt expectation: the two approaches to intermediary liability.

2.1. Description of both approaches.

When looking at the enforcement schemes presented in chapter two, one might notice that a fair amount of them involve escalating the intermediaries' fear of liability for the actions of their users, in order to have the former "do something" unspecified about the infringements or refrain from conducting their services altogether – an approach characterised in this work as "blunt expectation". Fitting examples of such enforcement schemes would include all modes of imposing civil and criminal liability on the intermediaries, covered in sections 3.1.1 and 3.2 of chapter two, respectively. For the policymakers, following the blunt expectation approach further would be tied to changing the law, in order to increase the penalties (ie. "the threat factor"), ramping up the enforcement efforts based on the law as it stands, and/or increasing the visibility of such efforts.

On the other side of the conceptual line lies the stance labelled in this thesis as the "specified request" approach. The notion behind it is that instead of crudely expecting the ISSPs to prevent the infringements from taking place, the legal systems could require the former to implement specific procedures or elements of infrastructure, with the liability arising not from the infringements of the users, but from the lack of compliance with the identified requirements.

[1056] *A Digital Single Market Strategy for Europe* (2015) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2015) 192, at 12.

In contrast to blunt expectation, the degree of reliance on the specified request approach is lower and less apparent. Throughout the EU, the ISSPs are still mostly subjected to some form of the former; nevertheless, there are some signs of the latter scheme being endorsed. An example of such a sign could be seen in the UK's usage of ISP-oriented blocking injunctions. If we look at the Newzbin 2 injunctions,[1057] the streamlined process of obtaining them and the lack of attempts to make the defendant ISPs liable in damages seem to be drawing this line of UK enforcement closer to the specified request approach. Demands furthered in, for example, *Scarlet Extended*[1058] and *Netlog*,[1059] if they would be more precise and presented in a more cooperative manner, could be another similar example.[1060]

The argument furthered in this chapter, and in this whole thesis, is that the specified request approach is a significantly better option, and that it should be implemented on the EU level, to a much deeper extent than the incidental examples presented in the preceding paragraph. It is submitted that this approach is better at the general, conceptual level, and that the discussion of the attached set of proposed specific requirements could lead to an improvement of the shortcomings associated with the online content regulation policy permeated by the blunt expectation approach. Due to the time and space constraints, this chapter by no means attempts to provide a complete answer all questions and concerns arising on the path of the policymakers wishing to design and implement a complete, worthy specified request system; however, it provides a valuable analytical road-map of the key decisions which should be taken in such a situation, the factors affecting such decisions, and - where feasible - suggests the more promising paths towards the desirable solutions. Lastly, it is not suggested that the specified request approach is a cure-it-all solution to the four types of infringing content

[1057] See section 3.1.2.3.1 of chapter two.
[1058] *Scarlet Extended v SABAM*, supra fn. 105.
[1059] *SABAM v Netlog*, supra fn. 103.
[1060] Though it has to be kept in mind that without appropriate guidance, effect-based website blocking injunctions incorporate conceptual elements of the blunt expectation approach, see the discussion of the *UPC Telekabel* case in section 2.2 of the current chapter.

covered in this thesis, but that it could provide for a major, composite improvement to the challenges they pose.

In order to support those statements in a clear and organised manner, this subchapter adopts the following structure. Section 2.2 compares the specified request approach to its blunt expectation counterpart on a general, conceptual level, discussing their merits and flaws. Section 2.3 presents a set of requirements which could be recommended for adoption within the specified request approach. Finally, section 2.4 discusses how the specified request approach could be implemented within the legal and institutional framework of the European Union.

2.2. Which approach to intermediary liability is conceptually better?

There are several key arguments speaking in favour of endorsing the specified request approach over its blunt expectation counterpart. Firstly, there is the advantage in effectiveness and efficiency, both being crucial concepts in this branch of law-making, as it was argued in chapter three.[1061] A scenario in which each ISSP is required to deal independently with the infringements on its own, to design, implement and operate the procedures aimed at tackling various kinds of infringing content appearing on its service, is less efficient than a scenario in which resources dedicated to devising and updating the anti-infringement measures are "pooled" together at a single organisation responsible for this task.[1062] While each intermediary might be slightly different in terms of its architecture, centralisation of the design process could nevertheless bring about an increase of its efficiency, as well as of the quality of the enforcement measures, or at least of their core elements. It is worth adding that small or start-up intermediaries, unable to dedicate the necessary

[1061] See sections 1 and 4 in particular.
[1062] See section 2.4 of chapter five for the suggested characteristics of such an organisation.

resources for designing and updating their anti-infringement arsenal, might receive a particularly significant benefit in this context.

Another argument in favour of the specified request is a twofold boost in legal certainty. While there is no express right to this value which could be discussed in the balancing section of chapter four, it is still a crucial quality of a desirable system of regulation. To demonstrate its presence in the regulatory discussion at hand: the Council of Europe's recommendation from 2007, focused on the cyberspace setting, urged the Member States to establish "the boundaries of the roles and responsibilities of all key stakeholders within a clear legal framework (…);".[1063] Furthermore, as Bitton rightly noted, general outlines of the intellectual property enforcement measures are not sufficient when it comes to online content regulation[1064] – and it is argued that this stance extends at this point to all four types of infringing content covered in this thesis. Finally, legal certainty, seen convincingly by the Attorney General in *Scarlet* as a concept descending from the rule of law,[1065] had its desired form expressed by Jones, who wrote that "our sense of predictability should be sourced from legal sources, which would be undermined if the sides of the balancing scales derived their weight from an extensive and unpredictable sample of legal, financial, commercial, ethical, technical or factual elements or justifications".[1066]

It is submitted that largely due to the presence of the blunt expectation variant, this undermining scenario gained presence in the intermediary-oriented sector of online enforcement. Without appropriate synchronisation, a landscape of diverse or diversely formed anti-infringement procedures emerged, a mosaic of procedures and technologies endorsed by the intermediaries wishing to

[1063] Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet, available at https://wcd.coe.int/ViewDoc.jsp?id=1207291
[1064] Bitton M, 'Rethinking the Anti-Counterfeiting Trade Agreement's Criminal Copyright Enforcement Measures' (2012) Journal of Criminal Law and Criminology 102 (1), at 116.
[1065] Opinion of AG in *Scarlet*, supra fn. 539, at [67].
[1066] Jones, supra fn. 1013, at 699.

avoid liability for the actions of their users. This leads to a significant, dual problem for legal certainty. Firstly, it is very difficult for the judiciary to be coherent in assessing whether, according to the law, each intermediary is doing enough to be, for example, "the diligent economic operator",[1067] one escaping liability. It is difficult to find specific, coherent guidance in case law on what procedures/actions should be expected from an operator of a cyberlocker, a streaming website, a blog platform, etc.

Secondly, the lack of such guidance could be seen as detrimental not only for the judges, but for the intermediaries themselves, who struggle to obtain a clear view of what is it that they should do in order to comply with the law. A perfect example of a recent case failing to provide the ISSPs' with such information is the earlier mentioned CJEU decision in *UPC Telekabel*.[1068] The Court's reasoning, devoid of much needed guidance with regards to the implementation of website blocking injunctions, has been criticised on this ground by multiple academics. Angelopoulos correctly stated that, "ISPs typically want precise orders to be laid out—they are much less eager to attempt to read that mind of the courts and apply guesswork regarding the legal rights of others, especially when their assessments will be subject to re-evaluation by the actual judicial authorities and a potential coercive penalty for themselves if they misgauge the balance;"[1069] the balance between their steps' effectiveness and these steps' impact on the human rights of users and ISSPs themselves. The *UPC* case leaves "all intermediaries except those whose case is identical to those already adjudicated in the dark concerning their rights and obligations".[1070] Husovec adds that "the court only delays the problem and creates a great deal of legal uncertainty that could have been prevented by rejecting, or at least limiting, the website-blocking injunctions in the main proceedings".[1071] Finally, following James - "(w)hile the UPC decision gives ISPs more freedom and flexibility to take their own steps to

[1067] *L'Oreal v eBay* (CJEU), supra fn. 620.
[1068] *UPC Telekabel*, supra fn. 995.
[1069] Angelopoulos, supra fn. 933, at 818.
[1070] Angelopoulos, supra fn. 933, at 815.
[1071] Husovec, supra fn. 1044, at 633.

address infringing content, many ISPs would probably prefer to be subject to a specific injunction which tells them exactly what they must do rather than risk falling short of what the court requires".[1072]

On the other side lies the specified request approach. In principle, within this variant, the judges know exactly which procedures an intermediary has to implement, depending on the service it is running, and intermediaries have much more clarity with regards to what is expected of them. It is true that then appears the question of whether the intermediaries properly implemented the specified requirements, but it is a lot more tangible and approachable one than its more generic counterpart emerging within the blunt expectation variant.

A further problem which developed in relation to the blunt expectation variant is that a single activity of an intermediary can oftentimes fall under more than one ground of liability – and it might be exceedingly difficult to predict which one of them is going to be relied on by the rightholders or the prosecution. While this difficulty is not inherent to the discussed approach to intermediary liability, it is one which evolved within it, and one which could potentially be remedied by the endorsement of the specified request approach.

Another principle which is given more adequate attention by this approach is the freedom to conduct a business. As discussed in section 3.3 of the fourth chapter, multiple enforcement schemes place a burden on online intermediaries, a burden which should be reduced as far as it is feasible. The blunt expectation approach, incorporating the effect-based demands, carries the risk of placing very significant, potentially unlimited strains on the ISSPs' resources. A generic result of, for example, "preventing one's service from being used for infringing purposes" might sound appealing but, in practice, the route leading to it might carry a considerable infringement of the right set out

[1072] James, supra fn. 1041, at 177.

in art. 16 of the CFREU - a threat recognised in both *Scarlet* and *Netlog*.[1073] The specified request takes away the risk of unlimited burden, and given the consideration process required for the implementation of this approach, it carries a lower risk of unjustly burdensome demands being made of the intermediaries. Additionally, the earlier mentioned notion of legal uncertainty suffered by the intermediaries (within the blunt expectation variant) can also be seen as going against the freedom to conduct a business, as pondering the perpetual question of "am I doing enough?" is likely to be resource-intensive in itself, due to the expertise it requires.

Finally, a shift towards the specified request could be seen as an opportunity for the creation of a legal enforcement framework which gives due attention to the relevant human rights at the design stage. Writing in the context of ISP blocking injunctions, the Advocate General Cruz Villalon stated that "(n)o [fair] balance can be said to exist in the case of an outcome prohibition not specifying the measures to be taken, which is issued against an ISP".[1074] At its core, this line of reasoning can be expanded to other categories of ISSPs, and to all four content types this thesis is focused upon. Outcome prohibition is closely tied to the blunt expectation approach; the latter's counterpart could provide better awareness and control over the impact of the enforcement schemes on human rights.

It could be argued that harmonising the design of the enforcement procedures endorsed by the ISSPs could open the specified request approach to a certain weakness, based on the idea that implementing a uniform set of measures which the intermediaries would be required to adopt could facilitate the circumvention efforts of the infringers wishing to, for example, bypass a website blocking injunction, confuse a preventive filtering system or avoid identification on a P2P network. Nevertheless, it seems that, even with this risk, the specified request is still more appealing than the blunt expectation

[1073] *Scarlet Extended v SABAM*, supra fn. 105, at [47] and *SABAM v Netlog*, supra fn. 103, at [46].
[1074] Opinion of the Advocate General Cruz Villalón in the Case C-314/12, at 85.

approach. To provide an example; concentrating resources on designing and updating a closed set of deeply sophisticated filtering technologies is likely to lead to the development of filters which can be bypassed only by a small number of fairly proficient infringers, with the vast majority of users being prevented from accessing the infringing content. And from the effectiveness' perspective, this could be a much more acceptable situation than the current one.

Concluding; the specified request approach excels over the blunt expectation approach by centralising the resources used for devising the best possible anti-infringement measures, tackling the "mosaic of measures" and "am I doing enough?" problems for legal certainty, reducing the threat to the freedom to conduct a business, and providing an opportunity to improve and maintain the adequate balance between all human rights involved. The risk of facilitating circumvention as a result of harmonisation exists, but it is nevertheless likely to be tied to a larger overall improvement in effectiveness.

2.3. Requests which could be made of various involved intermediaries.

In addition to the benefits of the specified request approach as a general concept, this chapter puts forward a set of procedures which different intermediaries could be required to endorse in a specified manner. The former are divided on two categories; the initial requirements, laying out the primary measures which ought to be taken towards the broadly understood end of removing access to the four types of infringing content (section 2.3.1) and the requirements focused on enforcing the other intermediaries' compliance with the initial requirements (covered in section 2.3.2, with other compliance-oriented measures). It has to be noted at this point that those two sections contain preliminary suggestions – in order for the specified request system to be effective, proportionate and workable, the design and implementation

process of both categories of requirements should allow for all involved stakeholders (rightholders and intermediaries in particular) to input and cooperate in a meaningful manner.[1075]

2.3.1. Initial, legitimising requirements.

While the discussion of each category of a legitimising requirement takes place in a dedicated section, there are some principles and disclaimers which concern all such requirements present in section 2.3.1, and which ought to be covered at this point. First of all, the key idea which should be kept in mind when laying out the legitimising requirements is that the wheel does not need to be reinvented; the crucial majority of the laid out procedures and steps which ISSPs could be asked to implement is based on the enforcement schemes presented in chapter two. While the latter could arguably be shaped and implemented in a better way (an underlying idea of this chapter), it is not really feasible to devise a new online enforcement landscape in a vacuum; though space for any novel approaches to enforcement should be left within the specified request framework.

Secondly, it should be recognised - given the discussion of the freedom to conduct a business in section 3.3 of chapter four - that an obligation which can be seen as reasonable for a large intermediary with plenty of resources might not be so for its smaller/start-up counterpart – as Husovec noted in the context of website blocking injunctions[1076] and Urban et al did in the context of the notice and takedown procedure.[1077] One way in which this distinction could be accommodated within the specified request system would be to rely on the definition(s) of small and medium enterprises (hereafter referred to as SMEs) set out in the Commission's recommendation from 2003. Its article 2 defines SMEs as "enterprises which employ fewer than 250 persons and which have

[1075] As it is further argued in section 2.4.1 of the current chapter.
[1076] Husovec, supra fn. 1044, at 633.
[1077] Urban et al, supra fn. 458, at 4.

an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million".[1078] Small enterprises are defined as those which employ "fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million",[1079] and the last category, microenterprises, are defined as those employing "fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million".[1080] The legitimising requirements (and potentially, their compliance-enforcing counterparts) could be curtailed/softened for the ISSPs matching one of the three categories. Additionally, criteria tied to the online setting (such as the amount of traffic received by a website) could also be involved in this mitigating exercise. Nevertheless, not all preliminary requirements would necessarily have to be adapted to the size of an ISSP.

Thirdly, every stakeholder group's interests and human rights should be taken into account when designing the preliminary requirements. This idea, which permeated throughout this work, is especially worth reiterating in the beginning of the current section. According to Ramalho's study, examining (inter alia) the degree of protection granted to various stakeholders by EU copyright law, "even though the exact margins may vary, the results show an EU copyright legislation that is partly industry-influenced, while other players seem to have fallen behind".[1081] While examining the merits of this conclusion is outside of this thesis' scope, it is clear that no category of stakeholders should be left behind when designing the obligations of intermediaries for all content areas.

Finally, when designing the specified requirements, the point of balance between over- and under-regulation is very narrow. Mindful of this, the Commission's report on the performance of the Memorandum of

[1078] Commission Recommendation concerning the definition of micro, small and medium-sized enterprises (2003/361/EC), art. 2(1).
[1079] Commission's recommendation on SMEs, supra fn. 1078, art. 2(2).
[1080] Commission's recommendation on SMEs, supra fn. 1078, art. 2(3).
[1081] Ramalho A, 'Copyright law-making in the EU: what lies under the 'internal market' mask?' (2014) Journal of Intellectual Property Law & Practice, 2014, Vol. 9, No. 3, at 224.

Understanding on Counterfeit submits that notice and takedown rules "should not be too prescriptive and must include certain mechanisms to deal with abuses of the system. Companies have come up with their own tailor-made methods to address infringements on their online sites".[1082] This chapter embraces the need to avoid the instances of over-regulation; however, it attempts to get as close to it as is justifiably beneficial and proportionate.

2.3.1.1. Notice and takedown.

The notice and takedown procedure (described in section 3.1.2.1 of chapter two) is the first one to be suggested for endorsement. The Memorandum of Understanding on the sale of counterfeit goods on the Internet[1083] (a voluntary agreement signed under the auspices of the EU Commission, a prominent example of an initiative leaning towards the specified request approach) described this enforcement tool as an "indispensable measure in the fight against the sale of Counterfeit Goods over Internet Platforms"[1084] – and it is argued that this statement holds true for all four types of infringing content.

Why is it worth to keep the notice and takedown schemes in place? Effectiveness-wise, as it was laid out in chapter three, they are vulnerable to several threats, such as the phenomenon of content returning onto the targeted platform (see section 2.1 of chapter three), the altsources migration (section 2.2) and the issue of technological circumvention (section 2.3). However, such schemes are likely to be effective enough to be a part of the enforcement landscape. It is very probable that a sizeable number of users can be prevented from finding or encountering the infringing content thanks to the notice and takedown. Moreover, this scheme carries a low cost on the public budget, and

[1082] *Report from the Commission to the European Parliament and the Council on the functioning of the Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet* (2013) EU Commission, COM(2013) 209 final, at 8.
[1083] Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet (2011), available at http://ec.europa.eu/internal_market/iprenforcement/docs/memorandum_04052011_en.pdf
[1084] Memorandum on counterfeit trade, supra fn. 1083, at 3.

is likely to carry a fairly high social acceptance factor (on which see back to section 5 of chapter three).

As for the potentially negative impact on the human rights involved, a look back to chapter four (section 3) reminds us that notice and takedown might be carrying certain side effects of this kind. Not really for the right to private and family life, but for the freedom of expression and the freedom to conduct a business. To remind; the former might be impaired through the direct removal of access to legitimate/potentially legitimate content (caused by inaccurate/malicious notices coupled with the inadequate assessment of content by the intermediaries, or by the reasoning in the Costeja case) or through the removal of access to infrastructure facilitating the spread of legitimate information (impairing the users' ability to exchange legitimate content, as well as the intermediaries' right to facilitate such an activity). As for the latter human right, processing the notices of infringement takes time and resources and as such constitutes an interference with the freedom to conduct a business of an intermediary burdened with this task.

Nevertheless, the balancing exercise conducted with those risks on one hand, and the interests of the rightholders harmed by the infringing content on the other, coupled with the fact that such risks have the potential to be mitigated, would seem to suggest that notice and takedown should be at least seriously considered as a part of the specified request approach. Urban et al's major study focused on the discussed enforcement scheme supports this position, by stating in relation to the DMCA 1998 (US-based, founding legislation for the notice and takedown procedure) that "though it shows strains, the law continues to provide rightholders with a copyright enforcement alternative that is cheaper and easier to use than lawsuits".[1085] The following paragraphs discuss what should the form of the former within the latter be, and approach the ideas aimed at facing the challenges identified in chapters three and four. If we are to make notice and takedown an official, mandatory condition for the

[1085] Urban et al, supra fn. 458, at 3.

chosen ISSPs' presence in cyberspace, this specified request has to be thought through in a robust manner.

The first question that is encountered in this endeavour is whether the initial obligation to operate a notice and takedown scheme should be placed on the intermediaries hosting the content, intermediaries indexing such intermediaries, or both. The conceptual base of the specified request, aiming to avoid blocking access to an intermediary who complies with the initial requirements, indicates that only the hosting intermediaries (or those holding a function closest to hosting – see the next paragraph) should be required to operate an N&T regime as an initial requirement. ISSPs indexing other ISSPs could be asked to cease doing so within the framework of compliance-enforcing requirements (see section 2.3.2 of the current chapter). However, it is submitted that – despite the fact that focus should be placed on the content's hosts - the indexing services should also be asked to maintain a notice and takedown procedure. This is due to the fact that reliance purely on compliance measures might be not be sufficiently prompt when, for example, volatile privacy-infringing information or a freshly released movie are concerned.

Therefore, the following intermediaries who appeared in chapter one should be asked to implement (or maintain) the N&T procedure:

- Cyberlockers.
- Streaming websites.
- Auction websites.
- Social media websites.
- Forums.
- Blogs.
- Torrent-indexing websites.
- Usenet-indexing websites.
- Search engines.
- Any other categories of relevant intermediaries which might arise in

the future.

The next aspect to consider is whether (in addition to the notices aimed at a piece of infringing content) there should be a possibility of aiming the notice at the account of a user who uploaded the said content. It is submitted that this should be an option – for all four content types - with the need for more complex (both in terms of amount and quality) evidence being taken into account. As discussed in section 2.1 of chapter three, shutting down an account might have a deterring effect, its basis ranging from sheer annoyance to the loss of key information or online personality. The Memorandum of Understanding dealing with counterfeit trade online supports this enforcement approach, in relation to the accounts of counterfeit sellers:[1086] though admittedly, the report on the Memorandum's performance states that "seller-based notifications are seen as cumbersome, as they almost always require additional offer-by-offer investigation before a decision can be taken".[1087] This burden, however, can be seen as justified by the reasons given in the same report, where it underlines the need for the human assessment in deciding on the gravity of actions undertaken against an allegedly infringing account – "(a) seller obviously acting in bad faith may be banned right away, while a repeat infringer whose first low-scale infringement occurred long ago may be warned again before the account is suspended".[1088] The report's list of factors guiding this assessment is worthy of being embraced by this chapter and contains the following: "the severity of the policy violation, the number of alleged infringements, repeat infringement, period of time since prior infringement, seller feedback, language that indicates clear intent, scale of legitimate business, as well as other more suspicious behaviour, such as efforts to avoid detection".[1089]

Moving onwards, there is an option of specifying the form of the infringement notices which the listed ISSPs are obliged to process. As the CJEU noted in

[1086] Memorandum on counterfeit trade, supra fn. 1083, at 3.
[1087] Report on the memorandum on counterfeit trade, supra fn. 1082, at 9.
[1088] Report on the memorandum on counterfeit trade, supra fn. 1082, at 11.
[1089] Report on the memorandum on counterfeit trade, supra fn. 1082, at 11.

the case of *L'Oreal v eBay,* such notices "may turn out to be insufficiently precise or inadequately substantiated"[1090] – and perhaps, this danger could be mitigated. The earlier mentioned Memorandum suggests that "notifications should be limited to necessary information, such as a clear identification of both the reporting party and the identification of the specific Offer of the Counterfeit Good. They should also contain a clear allegation that the Offer in question concerns a Counterfeit Good".[1091] Sets of suggestions akin to this one could be drafted for each type of infringing content and each type of an intermediary, wherever distinct treatment would be beneficial. Additionally, the notice's design could incorporate a field focused on factors nullifying the infringing character of information, such as exceptions or defences.

Another area of recommendation could be tied to the inherent differences between the four discussed content areas, and the impact of such differences on the performance of notice and takedown regimes. There is a danger that if the specified request system was to embrace a uniform, *fully* content type-neutral notice and takedown procedure, negative consequences could arise with regards to this measure's effectiveness, human rights impact and more.

This risk is explored in depth by Senftleben,[1092] in the context of copyright and trademarks – content areas which, in this thesis, could be seen as very close to each other due to both of them being intellectual property rights. However, as the cited author rightly notes, the two rights differ significantly when it comes to the aim and nature of the protection they offer. Copyright offers more direct protection from acts such as unauthorised reproduction or communication of work to the public. Trademark law, on the other hand, is more contextual in nature and does not protect the registered sign *per se*; the sign must be used in the course of trade[1093] and as Senftleben writes, "(t)rademark protection only concerns particular trademark functions, such as the (…) identification function, the quality function and the communication function".[1094]

[1090] *L'Oreal v eBay* (CJEU), supra fn. 165, at [122].
[1091] Memorandum on counterfeit trade, supra fn. 1083, at 3.
[1092] Senftleben M, 'An Uneasy Case for Notice and Takedown: Context-Specific Trademark Rights' (2012) available at http://ssrn.com/abstract=2025075
[1093] See art. 5 of the Trademarks Directive, supra fn. 156.
[1094] Senftleben, supra fn. 1092, at 10.

Hence, copyright offers a broader monopoly than even a well-established trademark with a reputation behind it.[1095] This can be justified by the lack of need to provide brand designers and owners with the same incentive to create as the authors of intellectual creations protected by copyright.[1096] Consequently, "(a) horizontal notice and takedown standard covering both copyright and trademarks will therefore inevitably be either too low a threshold to reflect the limits of trademark protection (…) or too high a threshold to encompass the more general rights granted in copyright law (…)".[1097] Furthermore, the different sets of exceptions present in copyright and trademark laws exacerbate the presented problem, with the latter containing more contextual exceptions as well (for example, the right to resell, or the right to inform about one's services).[1098] According to Senftleben, a trademark-focused notice and takedown procedure has to take into account both the scope/aim of protection and the exceptions peculiar to this content area.[1099] And while further comparative work of this kind cannot be conducted in this section due to time and space constraints, the same conclusion is likely to be true for each of the four content types covered by this thesis.

On this note; certain steps could be taken in relation to the process of assessing the infringement notices. For example, in order to alleviate a part of the burden tied to researching the answer to the question of whether the content complained of should be removed, and to enhance the likelihood of intermediaries taking into account the human rights dilemmas presented in chapter four, a special repository of corresponding legal knowledge could be established as a part of the changes introducing the specified request within the EU enforcement framework. Such a repository, run by a dedicated, EU-wide body,[1100] could give attention to the various types of infringing content (the discussed four to begin with), various forms of content (as the assessment differs depending on whether one deals with a video, music file or a fragment

[1095] Senftleben, supra fn. 1092, at 7.
[1096] Senftleben, supra fn. 1092, at 12.
[1097] Senftleben, supra fn. 1092, at 15.
[1098] Senftleben, supra fn. 1092, at 16.
[1099] Senftleben, supra fn. 1092, at 20.
[1100] The proposed form of which is described in section 2.4 of the current chapter.

of text), as well as various factors negating the infringing character of the content complained of (such as the copyright exceptions or defences to defamation[1101]). Additionally, apart from setting out those components from the EU law's perspective, the repository could also contain sections focused on each Member State, to take account of the laws distinct to each one of them.

It would also be beneficial if the intermediaries were to endorse a two-step approach, based on, first, assessing the probability of infringement and, secondly, considering the presence of factors nullifying the infringing character of content. Following Urban et al, such an approach should also be based on consistent human review, with automated processing of notices being significantly limited.[1102] However, even if the intermediaries were to be obliged to endorse such an approach as a part of the specified request system, it is exceedingly difficult to imagine how their compliance could be appropriately verified, even during the course of the appeals procedure. A mark of this difficulty lies on the US decision in *Lenz v Universal* (2015), where it was held that before submitting a takedown notice, the copyrightholders have to consider fair use; however, it was also held that they would only be liable in damages if it is proven that they acted in bad faith and knowingly failed to take fair use into account when submitting the notice.[1103] Proving these factors against an intermediary might be exceedingly difficult and burdensome for the claimants, especially when they are an average citizen. It seems that the discussed two-step approach could be included as a preliminary requirement, provided that the evidence of compliance (for the procedures described in section 2.3.2 of the current chapter) would be gathered in a manner devoid of an unacceptable interference with the intermediary's freedom to conduct a business and both users' and intermediary's right to privacy.

[1101] Covered in section 3.2.1 of chapter four.
[1102] Urban et al, supra fn. 458, at 3.
[1103] *Lenz v Universal* (2015) United States Court of Appeals, Ninth Circuit, 801 F.3d 1126, at 1137 and 1138.

The next idea related to the form in which N&T should be implemented within the specified request is a controversial one, and relates to the notion of efficiency. The question here is: should we require the ISSPs to process a set amount of notices in a set amount of time? By way of example; in 2015, the German government signed an agreement with Google, Facebook and Twitter, providing that those companies will remove hate speech-infused content within twenty-four hours of the notification (using German law, not the site's terms and conditions, as the basis for assessment).[1104] Indeed, the Memorandum of Understanding on Counterfeit states that the "Internet Platforms commit to offer efficient and effective NTD, which should be accessible through electronic means"[1105]; would not it be better to replace such an imprecise commitment with a precise, enforceable obligation?

There are several factors to consider in this regard. Firstly, what should be the formula endorsed? X notices to be processed in Y time seems to be the instinctive choice; however, in order to preserve fairness, this equation would have to take into account factors such as the size of an intermediary, the amount of notices of infringement its service is likely to attract, the type of infringing content likely to be involved (it may take a different amount of time to process, for example, a notice concerning defamation than one concerning copyright) and the form of content (assessing the information conveyed through text may take a different amount of time than evaluating a music or video file). Another base option is to request that, for example, for each 100X notices received, X have to be processed within Y time.

There are, nonetheless, certain risks tied to this approach. The first one is that it might prove to be nigh impossible to accurately pinpoint specific lines of guidance such as, for example, "a cyberlocker, processing X terabytes of transfer each month, is to process at least Y notices of copyright/trademark/privacy/reputation infringement in Z time". Cases differ

[1104] See http://www.bbc.com/news/world-europe-35105003
[1105] Memorandum on counterfeit trade, supra fn. 1083, at 3.

from one another; one might be a clear cut, straightforward case, while assessment of the other might take a much larger amount of time. Furthermore, it might be that one large rightholder (for example, a copyright enforcement agency) fills up the monthly quota with its notices, leaving other (oftentimes smaller) rightholders without the added (lawful) pressure on the intermediary. Finally, this specified request could be used for malicious competition practices, such as flooding a competitor with notices, in order to make it default on its obligation of running the N&T in the manner described.

All things considered, it would be unwise to adorn the notice and takedown procedure with a simple "do X per Y"-type obligation. However, a careful, deeper study, taking account of the factors described in the previous two paragraphs, and involving a significant period of consultations with the ISSPs, could lead to the finding of the right formula, one worthy of being submitted to the intermediaries.

Another aspect of the N&T which could be considered here is the appeals procedure. It may be argued that every ISSP operating the N&T should couple it with an adequately streamlined appeals procedure, in order to mitigate the potential interference with the freedom of expression.[1106] The appeal process should be efficient and user-friendly; this could, at least partially, be achieved through a simple pop-out window along the lines of "your content was removed, would you like to appeal, if yes, then on what basis (choose A, B, C, D or other)" – with an affirmative response meeting the eye of an appropriate employee. While this adds to the burden placed on the ISSPs' freedom to conduct a business, the right to a fair trial and the freedom of expression are arguably more important where it comes to the provision of the possibility of appealing the potentially inaccurate removals.

[1106] Discussed in section 3.2.1 of chapter four.

One of the frequently mentioned difficulties of using the N&T is how time-consuming it is to locate the infringing content in the first place. And if we look at platforms without internal search facilities, such as, for example, cyberlockers, this task becomes even more burdensome, pulling the rightholder closer to the point of diminishing returns.[1107] The question faced in this paragraph is whether the specified request's take on this enforcement scheme should require the presence of such facilities from various ISSPs in order to facilitate the rightholders' task of pinpointing the content striking at their interests. Given that such facilities would most likely be text-based, it should be noted that their effectiveness would be challenged by the same concerns as those encountered by the keyword filters, as described within the context of the *Atari v Rapidshare* decision.[1108] On the other hand, it could be argued that privacy-infringing and defamatory content are fairly susceptible to being found through internal search facilities (especially when the former are aiming at a single named person or entity). However, requiring the ISSPs to operate them could lead to a conflict with the right to privacy; users might wish for their files to be simply hosted, without being found through the hosting platform or even in any other way. Consequently, at this stage, the inclusion of the described search facilities is rather discouraged.

A supplementary step, also aimed at alleviating the burden of locating the infringement could be to develop and make publicly available a piece of software aimed at performing this activity. Currently, a fair amount of companies and anti-piracy organisations rely on such programs before filing the resulting notices of infringement. For example, BREIN (the Dutch anti-piracy body,) claimed that its infringement-searching software "removed more than fourteen thousand files at cyberlockers and 1,500 on YouTube".[1109] The "specified request agency" could be tasked with designing and spreading such a program(s), which could be especially beneficial for the smaller rightholders, who do not have the resources and technology of their larger counterparts.

[1107] Discussed in section 4 of chapter three.
[1108] Supra fn. 49, covered in chapter two, section 3.1.2.2.
[1109] See http://anti-piracy.nl/nieuws.php?id=320 (in Dutch).

Such a piece of software, while requiring substantial discussion and testing, could also be set to accommodate all four categories of infringing content. That being said, it should not accommodate the option of sending notices for the detected content automatically, due to the risk of inaccurate notices impairing the freedom of expression.[1110]

Further demands could be made with respect to the users' ability to report the presence of infringing content on the platform. The Memorandum of Understanding dealing with counterfeit trade contains a commitment to facilitate the users' ability to identify and report rogue sellers and their offers. It could be argued that such a mechanism should be further specified and applied in other areas of infringing content.

Moving on, it should be decided whether the notice and takedown procedures should endorse the so-called "notice and stay down approach", based on the intermediary's duty to prevent the illicit information it was notified of from reappearing on its platform. This author is of the opinion that while certain narrow, liability-wise finite forms of content filtering should be considered, the described approach should be dismissed, just as it was in the French case of *Société des Producteurs de Phonogrammes en France (SPPF) v YouTube* (2013).[1111] In those proceedings, the Paris Court of Appeal stated that there is no obligation for providers of hosting services to prevent the re-appearance of IP-infringing content they were notified of, and which they took down. Otherwise, such a duty would equate to the breach of art. 15 of the E-Commerce Directive – as well as, it should be added, to a disproportionate interference with the freedom to conduct a business. Furthermore, such a duty would pose a range of threats to the freedom of expression and privacy.[1112]

[1110] See section 2.3.1.2 of the current chapter for further discussion of software entailing automatic removals.
[1111] Decision of the Paris Court of Appeal of 21st June 2013.
[1112] As they were described in sections 3.1.2, 3.2.2 and 3.3.1 of chapter four.

Finally, it could be argued that in order to prevent the repeat infringers from spreading infringing content, the intermediaries should be required to implement certain steps, such as blocking the IP address of a persistently infringing user. The counterfeit Memorandum contains a provision reflecting this line of reasoning, where the operators commit to undertake their "best efforts" aimed at preventing the reregistration of repeat offenders whose accounts were shut down.[1113] However, relying on the IP addresses for this purpose encounters difficulties similar to those arising in relation to, for example, the graduated response schemes. These include IP addresses being changed, hidden or masked, or other users of the repeat infringer's connection being collaterally refused access. Nevertheless, given an appropriate appeal procedure, the discussed mode of response to persistent offenders could be introduced as a preliminary requirement.

2.3.1.2. Content filtering measures.

After notice and takedown, the second enforcement approach which could be considered as an initial requirement within the specified request approach is that based on the diverse landscape of software-based, content filtering measures, introduced in section 3.1.2.2 of chapter two. In contrast to the former scheme, they have caused much more controversy in the online enforcement debate. Most relevant intermediaries operate some form of notice and takedown; this is much less often the case for filtering procedures. It is quite telling how the Memorandum on Counterfeit is lacking when it comes to the agreements concerning specific filtering measures to be implemented by the operators. The document states that the latter "commit to take appropriate, commercially reasonable and technically feasible measures, taking into consideration their respective business models, to identify and/or prevent proactively the sale of Counterfeit Goods, especially obvious Counterfeit Goods, and to prevent such goods being offered or sold through their

[1113] Supra fn. 1083, at 6.

services".[1114] This collection of broad terms definitely describes the desirable characteristics of filtering systems, but it does not bring us closer to the specific shape the latter should take. Moreover, the cited paragraph is supplemented by a crucial phrase, reflecting inadvertently the spirit of the blunt expectation approach - "(t)he measures taken by Internet Platforms shall be at their discretion".[1115] Indeed, the place of filtering measures within the legal framework of the EU is a difficult and unclear one. As it was shown in sections 3.1.2.2 and 3.3.2 of chapter two, European law provides online intermediaries with extremely little guidance on how should they design their filtering systems (and whether they have to implement them at all).

In a move towards precision and legal certainty, the following paragraphs will attempt to face the question of: "what form should the filtering systems take?" While it is answered in the context of the proposal for a shift to the specified request approach, the analytical content of this section can, as is the case with many other parts of chapter five, be used outside of the blunt expectation vs. specified request approach debate.

Firstly, it is worth taking a step back and consider whether it is worth giving the content filtering measures, of any kind, a place in the reviewed enforcement arsenal. For this purpose, we may look back to chapters three and four. To start with the former; content filtering has undoubtedly encountered its share of effectiveness-related challenges. It is vulnerable to circumvention (such as changing the file names, meddling with the digital footprints used by the filtering software, or using the link-masking services), it does not have a strong deterring effect on the infringers, and it is troubled by the broader challenge of altsources migration. On the other hand, content filtering holds a particularly significant promise among the enforcement schemes; it has the potential to remove access to infringing content in a prompt and efficient manner, before such content causes much or even any harm at all. Moreover,

[1114] Memorandum on counterfeit trade, supra fn. 1083, at 5.
[1115] Memorandum on counterfeit trade, supra fn. 1083, at 5.

initiatives such as Content ID have shown that filtering schemes may have a significant impact on the amount of infringing content present on an online platform.

As for the human rights perspective, chapter four demonstrated how filtering systems might pose several threats. Firstly, filtering a platform in search of infringement might infringe the users' privacy, as it might open access to their content. The same human right comes under risk where the filtering systems collect information indicating users' online activities – a concern raised in *Scarlet*.[1116] As for the freedom of expression, the discussed enforcement scheme also poses a twofold risk; firstly, the filtering systems identify a piece of content but do not decide whether each instance of it is infringing or not; the system may not distinguish between legitimate and infringing content sufficiently well. Secondly, they may impair the intermediaries' freedom to be a facilitator of communications; as it was recognised in *Delfi AS v Estonia*.[1117] Finally the burden they place on the providers of online services can be seen as going against the freedom to conduct a business - the development and implementation of sophisticated filtering technology is likely to be far from cheap.

Nevertheless, the potential effectiveness and efficiency of filtering systems makes them a valid measure to be considered within the specified request approach. That being said, much more care and attention has to be given to requirements tied to this enforcement scheme, more than in case of their N&T counterparts. This is to ensure the lowest possible negative impact on the human rights listed in the previous paragraph, and the highest possible chance to disable access to infringing content effectively and efficiently. The following discussion of the content filtering schemes' characteristics is aimed at drawing out a path to those aims.

[1116] *SABAM v Netlog*, supra fn. 105, at [50].
[1117] *Delfi AS v Estonia*, supra fn. 873, at [94].

The first question that stands before this section is whether filtering should be conducted before or after some sort of action from the rightholders' side. The argument in favour of the former is that the rightholders would have to spend little if any of their resources – the Estonian Supreme Court embraced this reasoning in its judgement, leading to the *Delfi AS* case.[1118] Furthermore, the Grand Chamber of the ECtHR stated in the appellate judgment to the latter decision that "where third-party user comments are in the form of hate speech and direct threats to the physical integrity of individuals, as understood in the Court's case-law, the Court considers (…) that the rights and interests of others and of society as a whole may entitle Contracting States to impose liability on Internet news portals, without contravening Article 10 of the Convention, if they fail to take measures to remove clearly unlawful comments without delay, *even without notice from the alleged victim or from third parties*".[1119] It unfortunately remains unclear whether the Court would reiterate this position for the interests of copyrightholders, trademark owners, defamed parties, as well as those whose privacy was infringed.

On the other hand lies the argument that "notice-less" filtering should not be required of the ISSPs. It seems nearly-impossible to imagine a viable, balanced filtering system without any information (such as, for example, the digital footprints of their files or the defamatory message being spread) provided by the said stakeholders. The earlier mentioned report on the counterfeit Memorandum supports this reasoning, underlining the importance of rightholders and platform operators sharing information for the proper functioning of preventive measures[1120] – such as content filtering. Moreover, demanding the ISSPs to monitor their services for content which seems to be infringing is likely to be overly burdensome, going against both arts. 11 and 16 of the CFREU.[1121] Hence, it is submitted that the specified requirements should not include filtering systems devoid of any input from rightholders. It is true that a possible scenario in which blatant, most likely to be infringing

[1118] *Delfi AS v Estonia*, supra fn. 873, at [25].
[1119] *Delfi AS v Estonia* (Grand Chamber), supra fn. 1022, at [159], emphasis added.
[1120] Report on the memorandum on counterfeit, supra fn. 1082, at 10.
[1121] See sections 3.2.2 and 3.3.1 of chapter four.

content is noticed by the operators and not taken down is far from perfect; but in practice, requiring the intermediaries to act before any input from the rightholders (for example, with the actual knowledge requirement of the E-Commerce Directive[1122]) leads the former to putting horse-blinds on – as well as prompts long and uncertain inquiries into, for example, whether an editor of an online forum saw this or another post.

The second choice to be made is whether the filtering should occur pre- or post-upload. Writing in the context of trademark infringement on online auction websites, Friedmann argued in favour of the former option (supported by the product authentication numbers), due to its greater effectiveness and efficiency:[1123] endorsing it was also the first suggestion made by Arnold J in the UK limb of *L'Oréal v eBay*.[1124] It is in fact difficult to deny that preventing the infringing content from becoming accessible in the first place presents itself as a most desirable outcome: especially where volatile content is considered, such as novel, privacy-infringing or defamatory news. Furthermore, there are certain examples of effective pre-upload filtering schemes (supported by information provided by the rightholders) being put in place: Content ID, described above,[1125] being the key one. That being said, filtering of all content before the upload can be a) exceedingly burdensome for the ISSPs (especially those who do not have the resources matching those of the major companies), b) slowing down the performance of their services, c) damaging for freedom of expression, as the intermediaries might be less thorough in their content assessment due to the increased amount of files to investigate. Moreover, as it was mentioned in section 3.2.1 of chapter four, while certain types of infringing content are arguably quite visibly illicit (for example, major blockbuster movie, poor copies of Cartier watches), others pose much more of an investigative challenge (for example, a pornographic recording might not be revenge pornography, even if labelled as such). Furthermore, asking the intermediaries to keep track of the developments

[1122] See section 3.3.1.1 of chapter two.
[1123] Friedmann, supra fn. 745, at 154.
[1124] *L'Oréal v eBay* (UK), supra fn. 375, at [277].
[1125] See section 3.1.2.2 of chapter two.

within the society which could trigger the appearance of infringing content (for example, release of a new movie or a new Louis Vuitton handbag, celebrity photo leaks as well) and attuning their filtering systems accordingly is also likely to be exceedingly burdensome. Overall, it seems that pre-upload filtering could be requested of certain intermediaries; but only after a period of extensive studies estimating the filters' accuracy, operational costs and impact on privacy, with the latter desirably being non-existent.

Thirdly, the filtering schemes could be – or, to submit without delay, should be - differentiated with regards to the form of content filtered. Text, image, sound – different carriers of information may require a different way of examination, for both humans and computer programs.[1126] It is worthwhile to consider those media types in greater depth.

Text-based filtering is definitely a subject of consideration in the current enforcement debate; for example, the Memorandum on Counterfeit contains an agreement concerning the provision of keyword lists to the intermediaries, in order to assist their proactive measures.[1127] All four content areas contain infringing information which might be tied to certain words or combinations thereof; consider "Underworld the movie stream free", "cheap Louis Vuitton bag", "Jennifer Lawrence leaked photos" or "Jameel supporting Al-Qaeda". However, this approach has certain key concerns surrounding it. Firstly, effectiveness – in *Delfi AS*, it was stated that on its own the ISSP's keyword filter was an insufficient method of protecting the claimant's reputation.[1128] It did not prevent the comments in question from appearing on the page. In fact, as it was noticed, for example, in the *Atari v Rapidshare* case covered in section 3.1.2.2 of chapter two,[1129] the keyword filters are susceptible to simple forms of circumvention, such as naming the file "L.o.xxx.t.12.r.M00.v.i3" as opposed to "Lord of the Rings Movie". Additionally, overblocking is a

[1126] Though one could argue that for a machine, it might be different kinds of zeroes and ones.
[1127] Memorandum on counterfeit trade, supra fn. 1083, at 4.
[1128] *Delfi AS v Estonia*, supra fn. 873, at 87
[1129] *Atari v Rapidshare*, supra fn. 49, at [32].

particularly serious concern for this type of media, as focusing on even a carefully chosen set of words might lead to the removal of access to legitimate content (especially where removal of access occurs automatically, without human assessment – see the paragraph following the next one for the discussion of whether this should be warranted). As a result, it seems that the most appropriate path is to put keyword filtering into the specified request arsenal, but only in a supportive and detecting role, as opposed to being the key measure entailing automatic removal of access to content. Detection would have to be followed by examination conducted by a suitably prepared human person.

As for the filtering of audio, visual or audiovisual files, it is worth underlining the existence of filtering software capable of locating them. Good examples here would be the Content ID system on Youtube[1130] and further audio identification programs developed, for example, by Audible Magic, a company whose products are used by companies such as 21st Century Fox, Dailymotion, EMI, Mediafire, or Viacom. Despite the visible difference between a music file, an image and a video, such programs function in a similar manner to that of Youtube's Content ID – there is always a digital fingerprint created (in the form of a so-called hash), against which other content is verified. That being said, it is potentially possible to mislead the filters of this kind, by changing, for example, the size of the image, for it may change the hash. Overall, while there is a burning need to bring much more empirical/technological research into the process of answering the question of whether the Content ID-type filters should be a part of the specified request approach, the initial answer submitted in this thesis is affirmative: they should be, on a multitude of platforms, with databases of reference files being potentially run by the public authorities. As Valgaeren and Roland indicated, while Youtube can be commended for its use of Content ID, it should also be considered whether other ISSPs can/should implement this enforcement mechanism on their services.[1131] As we can see from the list of Audible

[1130] Described above, in section 3.1.2.2 of chapter two.
[1131] Valgaeren and Roland, supra fn. 631, at 222.

Magic's list of clients, apart from streaming websites (Dailymotion), it also contains at least one cyberlocker (Mediafire); which indicates the potential for broader application of this technology. That being said, adoption of Content ID-like technology within the specified request approach should depend on the presence of findings showing that the proposed filters would not unduly impair the right to privacy, the freedom of expression, and the freedom to conduct a business, in the manner described in sections 3.1.2, 3.2 and 3.3.1 of chapter four.

Moving further, a choice appears between filtering systems which automatically remove access to the located content and systems which merely notify the rightholder/intermediary about the find. The former has the potential to be more efficient in removing access to infringing content, especially where vast amounts of scanned items are involved; that being said, this option exacerbates the threat of overblocking.[1132] On the other hand, requesting the endorsement of a system which has to involve a degree of human assessment before content is made unavailable is likely to be of much lower efficiency, as well as possessing a lower chance of blocking access to legitimate content in a prompt manner. There are two further concerns related to this variant. Firstly, assessment of content which does not qualify as "blatantly" infringing remains an (often time-consuming and difficult) challenge. Secondly, it might be quite difficult to verify whether an ISSP is actually adding the human assessment factor to its procedure.

Before a suggestion is made with regards to which option is better, the role and shape of the appeals procedure should be considered, as it might severely affect the impact of a filtering system on freedom of expression - in a manner similar to that described in the previous section focused on the N&T schemes. It could be easier to accept an automatic removal filtering system which allows the user whose content was filtered out to instantly submit an appeal, which is in turn examined by a human person within a given space of time, or

[1132] Covered above, in section 3.2.1 of chapter four.

automatically returned online if such examination did not occur within the prescribed period.

For the time being, it seems that merely detecting filtering systems should be included in the set of specified requests, provided that it is proven that they do not pose an unacceptable threat to the right to privacy and the freedom to conduct a business. If the automatically removing ones are to join them, they should receive a considerable amount of empirical researchers' attention beforehand, obtaining data on the effectiveness and the human rights impact of such filtering procedures and programs.

The next question in line is whether the specified requests tied to filtering systems should take into account the distinctions between various categories of infringing content. Such distinctions might be tied to the software required to detect each type of content, as well as the systems' operating costs and the degree of accuracy it offers (for example, when a digital fingerprint system in copyright is compared with a keyword-based system aimed at preventing the spread of defamatory news). For the moment, further research is required in order to decide whether and how should those distinctions be weaved into the specified request package, for example, whether certain filters should be used for specific types of infringing content.

So far, the discussed aspects of the filtering requirements focused on the idea of an ISSP filtering traffic on its own service. However, the case of *GEMA v Rapidshare*,[1133] invites us to consider the role of a different approach: one based on an intermediary looking for indexing information leading to the said intermediary's content. In the indicated case, the injunction obliged a cyberlocker to look for links (leading to the infringing content it hosted) on, for example, indexing services or social media. Similar obligations could be set with regards to streaming websites, social media or forums. Should they

[1133] See section 3.1.2.2 of chapter two.

be? The proposed answer to this question is no; the potential for unlimited burden on the intermediary is too high, and it is more reasonable to narrow down the actions requested to the service of the concerned ISSP.

The next question in line is whether the content filtering obligations placed on the intermediaries should limit the rightholders' filtering requests to the specific content harming their interests, or whether it should be possible to ask an ISSP to filter out a broader category of infringing content, for example, copyright-infringing music or privacy-infringing content in general. The suggested answer to this query (tied to the earlier explored choice between pre- and post-notice filtering) is that the latter option should be dismissed as too broad, risky and burdensome – attributes which could be seen as tied to the blunt expectation variant. The line of reasoning embraced in the *Fox v Newzbin* judgment[1134] and potentially, in art. 15 of the E-Commerce Directive (should the term "general" obligation be interpreted to denote the focus on a broad category of infringement), should be maintained and extended.

While the technologically-infused discussion of specific filtering programs has to be, regrettably, placed outside of the scope of this thesis due to time and space constraints, it is nevertheless worth considering a certain mode of filtering, namely the deep packet inspection (hereafter referred to as the DPI), which started to appear in the academic discourse surrounding content filtering. To bring back a definition which appeared in section 3.1.2 of chapter four: DPI is succinctly defined by Daly as "(…) a technology deployed at the level of Internet provision to decipher the content of the information that is travelling through the network".[1135] This incorporates examining the content of information packets, not at their endpoint (for example, the user's computer), but when they are heading to their destination.

[1134] And described in section 3.1.2.3.3 of chapter two.
[1135] Daly A, 'The legality of deep packet inspection' (2011) I.J.C.L.P. 14, at 2.

DPI can be seen as a successor of two earlier methods of filtering, namely the shallow packet inspection and packet pre-filtering. The former relies on the files' headers and other frontline data, such as the IP addresses of senders and receivers of information; the latter on filtering out the suspicious packets, while letting the others through without review. Such a triggering suspicion can be derived from, for example, the software signatures ascribed to viruses. According to Bendrath, DPI differs from its predecessors by offering "the possibility to analyse and discriminate Internet traffic in real time," and integrating these functions within a single piece of hardware.[1136]

While it was originally designed as a method of managing the network for the purpose of protecting the users from malicious programmes, deep packet inspection began to be considered as a method of filtering out the other types of undesired content, including the four covered in this thesis. However, there are certain concerns over such an extended use of DPI; as Daly argues, it seems "to generate *prima facie* privacy concerns, as data about users' behaviour on the Internet (which could also include sensitive data) is being monitored and used for various purposes".[1137] Moving forward in this line of reasoning, endorsing DPI within the specified requirements would require compatibility with the Data Protection Directive.[1138] Furthermore, Daly's call for transparency in the use of deep packet inspection should be echoed in this section with approval; this value could at least partially be attained via the ISSPs informing their users that DPI is endorsed by the service.

Should DPI be embraced by the specified request system? At this stage, it is suggested that until empirical research shows that the impact of this technology on privacy, freedom of expression and freedom to conduct a business is acceptable, that the earlier mentioned concerns are in fact

[1136] Bendrath R, 'Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection' (2009), Paper prepared for the International Studies Annual Convention New York City 15-18 February 2009, at 14, available at: http://userpage.fu-berlin.de/~bendrath/Paper_Ralf-Bendrath_DPI_v1-5.pdf
[1137] Daly, supra fn. 1135, at 8.
[1138] Daly, supra fn. 1135, at 8.

exaggerated, the answer should be no. It seems plausible to state that deep packet inspection of all content, involving automatic action (such as blocking) should not be allowed in cases where the only marker of infringement is a set of keywords. This position could be different for DPI tuned towards the digital fingerprints.

Finally, careful consideration has to be given to the exact extent to which technological solutions are to be imposed on the ISSPs. The essence of the specified request approach is that the ISSPs should not be simply asked to provide an effect; however, laying out the filtering software they are to implement with excessive precision, down to every last line of code, is unlikely to be the desired approach either. ISSPs know their services well, and there are plenty of good reasons why they would not like someone to get familiar with or meddle in their most internal infrastructure. In laying out the content filtering requests, exceptional care should be paid to the adequate amount of choice left for the intermediaries wishing to comply with the identified requirements.

2.3.1.3. Facilitating the identification of infringers.

The third category of specified requests discussed in this subchapter is built on those tied to the identification of infringing users.[1139] As section 3.1 of the third chapter argued on the basis of, inter alia, the study conducted by Adermon and Liang,[1140] providing the rightholders with such an option is key to obtaining the primary form of infringer-focused deterrence. Requests tied to the identification mechanisms can be divided on two, closely linked categories; those tied to the collection of user-related data, and those tied to its disclosure.

[1139] An enforcement challenge discussed in section 2.3 of chapter two.
[1140] Adermon and Liang, supra fn. 763.

Commencing with the former: the primary set of requirements could set out which types of data each type of an intermediary ought to collect with the identification requests in sight. Following the *Seitlinger*[1141] case, which invalidated the Data Retention Directive, this topic is open for discussion at the European level, which should be started by the recognition of a fact that various ISSPs have/can demand the access to different categories of data. Consequently, a data type-based order is endorsed for the purpose of this subsection.

The first type of data which could be collected are the IP addresses. In itself, this statement is far from novel – chapter two shows how prevalent this path of identification is for the enforcement schemes such as the infringer's civil and criminal liability, not to mention the graduated response, which basically depends on the collection and maintenance of P2P users' IP addresses by their Internet connection providers. It would be novel to develop a list of intermediaries who have to collect IP addresses, and implement it within the EU legal framework.

The second type of data which the ISSPs could be required to collect are the real names and addresses of their users. The connection providing ISPs are already obliged to do so by the earlier mentioned art. 6(b) of the E-Commerce Directive,[1142] some online services (such as Facebook) voluntarily endorse this approach, and there are traces of it in the Memorandum on Counterfeit, which states that the "Internet Platforms commit to take commercially and technically reasonable steps to request seller contact information and to verify this information, provided by sellers, in specific circumstances that warrant such identification, in order to gain a reasonable assurance of a seller's identity".[1143] That being said, there is little doubt that imposing such a requirement on further categories of intermediaries (such as social media, streaming and hosting websites, online forums, etc.) could raise serious,

[1141] Discussed in section 3.1.1 of chapter four.
[1142] Covered in section 2.3 of chapter two.
[1143] Memorandum on counterfeit trade, supra fn. 1083, at 4.

arguably justified concerns tied to privacy and data protection. Furthermore, it would entail a major upheaval in the realm of anonymising services (such as VPN providers) as the core of their business and the measure of their popularity is based on the lowest possible amount of user data collected. Should such data be collected, the VPN providers could be asked to disclose not only the names, but also (as O'Sullivan notes), for example, the credit card details of alleged infringers.[1144]

Having covered the collection of data, let us turn to the specified requests which could be made with regards to its disclosure. Yet again, there are ample examples of users' data already being legally disclosed in the EU for the purpose of locating infringers, primarily through court orders akin to the *Norwich Pharmacal* order[1145] or the one made in the *Promusicae* case.[1146] The Memorandum on Counterfeit also aims to facilitate such disclosure, when it proclaims that "(t)o facilitate legal actions and investigations into the sale of Counterfeit Goods, Internet Platforms commit to disclose, upon request, relevant information including the identity and contact details of alleged infringers and their user names insofar as permitted by applicable data protection laws".[1147]

What then could be further specified as a part of the reform discussed in this chapter? This question can be answered by putting forward three aspects of user data disclosure. Firstly, the standard of the identification request and its likelihood of being related to actually infringing content can be set out expressly: though going down this path should be backed by a significant amount of preliminary research. Secondly, the ISSPs can be required to respond to the ID requests within a specified amount of time, or process a certain amount of such requests in a given space of time; with factors such as the amount of overall traffic processed by the service provider or the type of

[1144] O'Sullivan, supra fn. 712, at 580.
[1145] *Norwich Pharmacal*, supra fn. 913.
[1146] *Promusicae*, supra fn. 322.
[1147] Memorandum on counterfeit trade, supra fn. 1083, at 5.

infringing content being taken into account. This solution is discouraged on the basis of factors similar to those which were mentioned in relation to the comparable notion proposed in the context of the notice and takedown procedure, in section 2.3.1.1 of the current chapter. Finally, the allocation of the identification procedure's costs (following the request) could be regulated – whether the burden should be placed exclusively on the intermediary (according to a UKIPO's report, it is most often the case for ISPs worldwide[1148]), shared with the rightholders (as is the case in the US[1149]) or reimbursed by the government (as is the case in France[1150]). At the moment, a detailed empirical assessment would be required to decide which of these costs regimes would be most appropriate and whether this should differ depending on the legitimate interests being infringed.

2.3.1.4. Providing for the right to reply.

Sometimes, the suitable remedy is not based on removing access to the discussed content or identifying the infringer; for example, it might be sufficient for the rightholder to place a reply next to the allegedly infringing piece of content, so that the latter is never seen without the former. Facilitating this response mechanism (which has not gained sufficient presence to be discussed in chapter two) can be seen as another obligation to be considered within the specified request approach.

The roots of this remedy can probably be found in the area of defamatory news articles, where a newspaper may be ordered by the court to publish a rectification of their previously published material. Moving closer to the context of this thesis, endorsement of this "right to reply" can be seen, for

[1148] *International Comparison of Approaches to Online Copyright Infringement*, supra fn. 703, at 4.
[1149] *International Comparison of Approaches to Online Copyright Infringement*, supra fn. 703, at 4.
[1150] *International Comparison of Approaches to Online Copyright Infringement*, supra fn. 703, at 4.

example, on the largest Polish auction website, Allegro.pl.[1151] While auction sites were thus far discussed in relation to trademark infringement, defamation can also occur there, particularly where seller reviews are considered; for example, a malicious user or competitor might describe the seller as untrustworthy, slow or unresponsive. Allegro allows the seller to post a reply to such comments, and, furthermore, has a corresponding dispute resolution mechanism, whereby if the seller and user come to an agreement, the allegedly defamatory review/comment receives an annotation informing the viewer about this fact and noting that such content is no longer valid. According to Collingwood, such an approach could reflect the position of the German law of defamation, where "the primary relief in respect of a claim in defamation is that of correction, in the form of reply and retraction, as opposed to damages, the latter being limited in amount given their subsidiarity to the discursive remedies available".[1152]

In terms of the freedom of expression, Allegro's policy provides a response to the concern over the removal of access to potentially legitimate information[1153] as the user's comment is not erased from the website, despite losing its main defamatory impact. However, it should be noted that the effectiveness of the remedy in question might differ when applied to other types of infringing content. If we take a copyright-infringing scenario of a movie hosted on a streaming website, the studies conducted by Adermon and Liang,[1154] as well as Lysonski and Durvasula,[1155] indicate that a mere side-notice informing the viewer of the illicit character of the video is unlikely to deter him from viewing it. Similarly, if someone is actually looking for counterfeit products on the shopping and auction sites, a corresponding notice is also unlikely to work: the case might be different if we take the right to reply as a warning for bona fide shoppers - then it might be a safe and efficient measure, provided that sufficient evidence of infringement is gathered before

[1151] See http://allegro.pl/country_pages/1/0/user_agreement.php#rule11
[1152] Collingwood, supra fn. 910, at 6.
[1153] Discussed in section 3.2.1 of chapter four.
[1154] Adermon and Liang, supra fn. 763.
[1155] Lysonski and Durvasula, supra fn. 770.

the reply is posted. As for the privacy-infringing content, Collingwood suggested that the discursive remedies of the law of defamation (such as the right to reply) should be applied within the realm of privacy.[1156] However, looking back to the privacy-infringing scenarios[1157] (which included a Facebook group portraying the site's users as prostitutes/promiscuous women, a revenge pornography website and a footballer's affair being made public via Twitter) it is difficult to see how a side notice from the rightholder could be of significant help in removing the privacy-infringing component of the discussed information. It could nevertheless serve as a softer, readily-available mechanism to portray the information in a different light, before the access to infringing information is removed; and for this reason, it is suggested that providing for the possibility of reply should be included in the set of legitimising requirements, for all four content types.

2.3.1.5. Graduated response within the specified request approach.

The graduated response scheme, described in detail in chapter two,[1158] can also be seen as a set of obligations which can be placed on the intermediaries; namely, the ISPs. Following the analysis enclosed in chapters three and four, it is feasible to begin this section by facing the question of; "is it worth it?" UKIPO's report declares that "(o)f the graduated response processes that have been implemented long enough to be assessed (i.e. FR and CA), stakeholders view these as being relatively successful. They point to the dramatic fall in numbers of notifications that are issued between different stages of the graduated response".[1159] However, as it was shown earlier,[1160] a fall in notifications is a very questionable criteria of effectiveness. While some measure of single platform deterrence may be achieved with this enforcement scheme, and some users might be redirected towards legitimate sources of

[1156] Collingwood, supra fn. 910, at 6.
[1157] Described in section 4.2 of chapter one.
[1158] Section 2.4.
[1159] *International Comparison of Approaches to Online Copyright Infringement*, supra fn. 703, at 5.
[1160] In chapter three, section 2.2

copyrighted content, graduated response is too fragile to be considered an effective, long-term strategy. Its current reliance on the IP addresses opens it to circumvention methods such as the use of VPNs and the P2P filesharing ecosystem is most likely to develop its architecture in a manner preventing the rightholders from simply entering a network and gathering the infringers' IP addresses.

In the human rights perspective, graduated response poses a certain amount of potentially negative impact. The right to privacy could be unduly impaired if the data linking users to IP addresses was to be misused, a risk inherent to all IP address-based identification measures. Freedom of expression may be harmed if copyright infringement reports are filed for legitimate or potentially legitimate content: however, this would be a significant concern only if the ISPs' verification procedures were to be highly dysfunctional. Finally, the impact on the freedom to conduct a business might be a noticeable concern, and empirical data on the ISP's burden of running various variants of graduated response is needed to assess this line of concern.

Overall, the evidence gathered in this thesis suggests that whether we consider graduated response in its more direct form (represented by the Digital Economy Act 2010[1161] or the HADOPI law[1162]) or in its softer, non-punitive aspect (embraced by the US Copyright Alert System[1163] or its UK counterpart, Creative Content UK[1164]), it is unlikely to be the satisfactory, long-term solution to copyright-infringing P2P filesharing. The perceived effectiveness of the graduated response does not seem to justify the costs and the human rights risks, and it is advisable to drive the search for adequate specified requests away from this enforcement approach. It is true that decentralised, infringing P2P filesharing remains a demanding regulatory challenge – especially if we envisage a future in which it occurs without an intermediary

[1161] DEA 2010, supra fn. 332.
[1162] HADOPI law, supra fn. 331.
[1163] Supra fn. 334.
[1164] Supra fn. 342.

who could endorse the earlier-described preliminary requests such as N&T or content filtering. However, the hard truth is that if such a vision was to materialise, the policymakers will have to face fundamental, immensely difficult questions about the structure of the Internet and the state's control over it. For the moment, the research conducted for this thesis suggests that within the specified request variant, it is better to eschew the graduated response schemes, and focus on the obligations such as notice and takedown and content filtering, reinforced by the compliance requests laid out below.[1165]

2.3.1.6. Prohibiting certain elements of the infrastructure.

The final category of obligations which could be implemented is likely to be the most controversial among the ones discussed in this section; and one which has not really been endorsed by EU policymakers yet. It is based on requiring the ISSPs to refrain from implementing certain components/mechanisms/services on their platform. As Friedmann wrote: "Lessig made clear in his book *Code and Other Laws of Cyberspace*, that code, or digital architecture, shapes law. But one can argue that it also shapes infringements".[1166] And, as a cyberpunk writer William Gibson wrote in one of his short stories - "the street finds its own uses for things".[1167] It could be argued that some elements of online services encourage or facilitate infringements so much that the law should prohibit them. The affiliate programs embraced by multiple cyberlockers[1168] can serve here as an example which could be subjected to the presented argumentation. Anonymising services could also be indicated in the same context. This includes the earlier mentioned VPNs, but also services such as the anonymous email platforms; especially given that one such platform, cock.li, had its servers seized in 2016

[1165] In section 2.3.2 of the current chapter.
[1166] Friedmann, supra fn. 745, at 152.
[1167] Gibson W, 'Burning Chrome' (1982) Omni, at 21.
[1168] Described in section 2.2.1 of chapter one.

by the German prosecution service, without any requests being made to cock.li's operator.[1169]

Overall, the policymakers should be very careful before outlawing the elements of ISSPs' infrastructure, so as to avoid significant harm to innovation, freedom of expression and public interest in general, as well as to prevent the backlash problem. Following down the discussed route could lead to the acceptance of the harmful line of claimant's reasoning from *Viacom v Google* - that Youtube's business model is "based on building traffic and selling advertising off of unlicensed content, [and] is clearly illegal".[1170]

2.3.2. Compliance and compliance-enforcing requirements.

It is clear that if the specified request model is to work, especially with the liability for users' infringements being parted with at certain point, the intermediaries' cooperation and compliance has to be ensured through a different path, one that strives to achieve the most required point of balance between being overly punitive and insufficiently effective. It is clear that the discussion on the shape of this path would be of crucial importance, and that the corresponding design process should include input from all relevant stakeholders, online intermediaries in particular. At this point, the author would like to commence this discussion by proposing a graduated response model[1171], with four tiers of response applying to ISSPs who fail to adhere to the preliminary requests ascribed to their service. Should one of the tiers fail to produce the desired effect, the following one would be triggered.[1172] Additionally, it is worth noting that those tiers oftentimes involve a provider of online services taking action against another intermediary – hence, the

[1169] See http://arstechnica.com/tech-policy/2016/01/cock-li-server-seized-again-by-german-prosecutor-service-moves-to-iceland/

[1170] See http://betanews.com/2007/03/13/viacom-files-landmark-copyright-case-against-google-youtube/

[1171] Not to be confused with the enforcement scheme described in section 2.4 of chapter two.

[1172] With the exception of the transition from the third to fourth tier, as the latter splits on two paths, depending on whether the targeted ISSP is located within the EU.

inclusion of the term "compliance enforcing requirements" in the title of this section.

2.3.2.1. Tier 1 – Warning letters.

The first suggested action to be taken if an ISSP is found to default on its "specified request" obligations is to send up to three letters notifying the intermediary of such derogations in detail, recommending the path to remedy them and describing the further tiers of response which await if the ISSP fails to adhere to the letter. Each letter should be separated by a fair amount of time, and provide an opportunity for a detailed reply. On the European level, the sender of those letters could be found in the body of the EU agency in charge of operating the specified request system – see section 2.4 of the current chapter.

2.3.2.2. Tier 2 – Disabling the revenue streams.

Should the letters fail to take effect, the first punitive tier of response could be activated. It reflects the so-called "follow the money" approach to tackling online infringements, which is supported (inter alia) by entities such as Google[1173] or the European Commission.[1174] Here, it would be aimed at disabling the sources of intermediaries' revenue, in order to induce the latters' compliance.[1175]

"Following the money" is most likely to be effective within the context of copyright, and for a good reason; while online piracy started out as more of an

[1173] *How Google Fights Piracy* report (2013) by Google, at 22, available at https://docs.google.com/file/d/0BwxyRPFduTN2dVFqYml5UENUeUE/edit
[1174] *Upgrading the Single Market: more opportunities for people and business* (2015) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2015) 550, at 15
[1175] See back to section 3.2 of chapter three.

idealistic, social phenomenon,[1176] it experienced an immense growth once money entered the system, in the form of advertising revenue, premium accounts and the earlier mentioned affiliate/reward programs. Consequently, as Lauinger et al wrote, "strategies against economically motivated actors may effectively target certain parts of the ecosystem [of online piracy]".[1177] Copyright-facilitating cyberlockers could be a prime example of such an actor. They mostly depend on the users' payments for financing and, hence, steps such as approaching PayPal and asking them to stop processing payments to the targeted website's account could potentially be effective. In fact, Lauinger et al noted that the one-click hosting services "are probably most vulnerable to antipiracy measures targeted at removing external sources of revenue".[1178] Other content areas also contain instances of intermediaries profiting from the infringing traffic, notable examples would include the websites focused on facilitating counterfeit trade (such as Akanoc[1179]) and the revenge pornography websites (such as IsAnybodyDown[1180]).

Another good example of the "follow the money" approach is the advertising blacklist operated by the PIPCU, a UK police unit mentioned earlier with regards to the domain name seizures.[1181] The blacklist is a part of an initiative dubbed "Operation Creative", and consists of a list of websites deemed to be "copyright infringing sites, identified by the creative industries and evidenced and verified by the City of London Police unit"; providers of online advertising services are encouraged to cease the provision of their services to such websites.[1182] The encouragement factor might be enhanced by the fact that the major bodies representing the advertising industry in the UK are partners to the Operation Creative. The PIPCU stated that the "pilot saw a clear and positive trend, with a 12% reduction in advertising from major

[1176] Inspired by the ideas laid out by Schultz, see section 3.2 of chapter three.
[1177] Lauinger et al, supra fn. 651, at 13.
[1178] Lauinger et al, supra fn. 651, at 12.
[1179] See section 3.2.2 of chapter one.
[1180] See section 4.2.1 of chapter one.
[1181] In section 2.3 of chapter three.
[1182] See https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/Pages/Operation-creative.aspx

household brands on the identified illegal websites".[1183] On the other hand, it is worth adding that the list itself is not made available to the public, which raises questions of legitimacy and transparency.

Another initiative in the similar vein, encompassing the activities of both advertisers and payment providers, was conducted by BREIN, the Dutch anti-piracy outfit. According to the organisation's report from 2013, "in 41 cases, payment providers provided BREIN with information to identify illegal sites and stopped servicing the operators of these sites".[1184] Additionally, "(m)ore than 100 advertisers also committed to stop advertising on sites propagating the unlawful supply of films, series, music, books and games".[1185]

There are several potential problems connected to the strategy based on cutting out the sources of revenue originating from the infringing traffic. Firstly, it can be exceedingly difficult to separate the profits coming from facilitating the spread of legitimate and illegitimate content. Secondly, as Lauinger et al pointed out, even if the more visible advertising companies were actually convinced/forced to cease conducting business with the "infringing" websites, there are alternative, "underground" advertising networks which might remain available; though it has been reported that they may generate lower revenue than mainstream advertising providers.[1186] The risk of diversification of income sources is another potential concern for the strategy in question, as is the presence of alternative payment systems, such as Bitcoin. Also, it has to be remembered that money is still not the only thing driving the operators of online services; exceptions such as The Pirate Bay continue to prove it.

[1183] See https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/pipcu-news/pages/city-of-london-police-call-for-help-tackle-cyber-crime.aspx
[1184] BREIN report, supra fn. 1109.
[1185] BREIN report, supra fn. 1109.
[1186] Lauinger et al, supra fn. 651, at 12.

While, conceptually, the PIPCU initiative (in itself) is still a part of the blunt expectation approach – as far as the targeted websites, not advertisers, are considered[1187] – it demonstrates one of the routes which the second tier of compliance enforcement within the specified request approach could take, and so do the other examples mentioned in this section. The earlier mentioned concerns about effectiveness do not seem to bar the "follow the money" component from being endorsed in this context; though certainly they should be empirically surveyed both before and after the potential introduction of the specified request system. Additionally, the issue of division on the revenue derived from infringing and non-infringing traffic is less of a concern where compliance with the specified procedures is the aim of the undertaken actions.

2.3.2.3. Tier 3 – Injunctions preventing the operators from running the service.

Should both letters and the revenue blockade fail, the non-compliant ISSP could receive a "yellow card" – a court order preventing it from operating its service until such time that it is confirmed that the derogations from the specified requests were adequately addressed. The order itself would not include any penalties for the lack of compliance, such as fees or prison sentences. Instead, an intermediary continuing to operate its service despite the described injunction would – after a suitable amount of time – face the fourth tier of response, described below.

2.3.2.4. Tier 4 – Access blocking and criminal takedowns.

The final tier of response is composed of last resort measures. By this time, the focus of the system is changed from inducing the ISSP's compliance to removing its presence in cyberspace. Certainly, should the intermediary begin to rectify its attitude towards the ascribed requirements, the tier of response could be lowered. However, until this happens, it is suggested that the non-

[1187] For the advertisers, it falls strongly into the specified request compartment.

compliant operators should be subjected to either or both of the following measures; the criminal law shutdowns (as described in section 3.2 of chapter two and on the example of the Megaupload shutdown[1188]) and the website blocking measures (discussed in section 3.1.2.3 of chapter two). The decision on which approach should be embraced within the EU could be made on the basis of the online intermediary's location; should it be located in one of the Member States (for example, by servers, domain name, or operators' presence), the criminal law measures could be enabled, due to the presence of reachable targets.[1189] In the absence of such presence, the ISSPs' service could be targeted by a range of blocking tools: which, in the former case, could also be used alongside the criminal path of enforcement.

Both modes of response could be refined, primarily in the manner reflecting the challenges ascribed to them in chapter three and four. While detailed deliberation on the details of such refinement could be the focus of a separate doctoral project, this chapter can nevertheless discuss some points of guidance on the adequate implementation of both fourth tier response mechanisms.

2.3.2.4.1. Last resort response - access-blocking.

The proposed approach to access blocking within the specified request approach is as follows. First of all, the dedicated body described in section 2.4.2 of the current chapter would maintain a list of all intermediaries who reached the fourth tier of response. Such a list would be communicated to all relevant ISPs operating within the EU, so that they block access to the rogue services. The actions which the former should take would be specified, in line with the conceptual underpinnings of the specified request as presented above.[1190] This could be seen as a reply to the concern raised by the UKIPO report in the context of blocking injunctions in France; its authors argued that

[1188] See section 2.2 of chapter three.
[1189] See section 3.2 of chapter two for the discussion of what those targets are.
[1190] See section 2.1 of the current chapter.

those orders "remain largely ineffective under current legal conditions", due to the rulings not specifying the actions which the ISPs and search engines should take following the decision.[1191] This new, EU-wide blocking system would not affect the national courts' ability to grant blocking injunctions against the same or other intermediary.

For the ISPs, the choice of the direct method of access blocking lies currently between IP blocking and DNS blocking – as Angelopoulos rightly states, "(i)t is hard to conceive of realistic blocking measures that might be applied by an intermediary that do not involve either domain name or IP address blocking, particularly if filtering obligations or other methods that involve monitoring are indeed to be seen as already ruled out by the *Sabam* case law".[1192] Following on the notion of effectiveness, it is suggested that the tier 4 access blocking should be focused on the IP addresses. Pure DNS blocking[1193] does not hold enough promise here, as it can be circumvented in too many ways described in section 2.3 of chapter three. As for the circumvention efforts aimed at IP blocking, they have to be accounted for: though it is difficult to indicate a clear path to mitigating them. The intermediaries' IP hopping practice[1194] can be negotiated with two primary paths; the first one is to chase after the new IP addresses (and add them to the list), in the manner akin to the BREIN agency, which (according to its report from 2013) removed 206 proxies used to circumvent The Pirate Bay blockade in the Netherlands.[1195] The downside of this strategy is evident, it is the hydra's heads' scenario, and getting briefly ahead requires time and resources, which not all rightholders might be able to dedicate. The second mode of response to the practice in question is to forego blocking measures for the sake of criminal enforcement, assuming there are valid targets for it available – for example, the operators or the servers. Nevertheless, it has to be remembered that not all ISSPs are

[1191] *International Comparison of Approaches to Online Copyright Infringement*, supra fn. 703, at 52.
[1192] Angelopoulos, supra fn. 933, at 819.
[1193] Ie. where the blockade takes place at the domain level, not where the domain names are used to implement an IP address-based block.
[1194] Described in section 2.3 of chapter three.
[1195] BREIN report, supra fn. 1109.

willing to play the cat and mouse game with law enforcement, and some degree of the deterrence effect might still appear as a result of access blocking, despite the concerns phrased out in sections 2.3 and 3.2 of chapter three.

As for the users' circumvention efforts, based on the use of proxy services and networks such as TOR or JAP (described in section 2.3 of chapter three), the situation is difficult to say the least. In the current legal climate, it is not really possible to simply outlaw the anonymising services and networks without undermining the strong protection given to anonymity in cyberspace.[1196] Asking the intermediaries implementing the blockade to go after the proxies themselves is inadequate, overly burdensome and disproportionate – and the decision of the Belgian Supreme Court endorsing this line of reasoning[1197] should be seen as such. However, it should be explored whether at least some operators of anonymising services could be obliged to implement the access-blocking list of ISSPs vehemently refusing to follow the specified requests ascribed to them. The difficulty in securing the formers' cooperation would lie in the likely decrease of an anonymising service's popularity, following the adoption of the blacklist. Then again, it should be kept in mind that not all users wishing to access a blocked website would use the discussed circumvention methods.

While Angelopoulos states (by reference to the studies accompanying one of the TPB cases covered above[1198]) that "existing data suggests no type of blocking has noticeable effect on actual numbers",[1199] it is submitted that, despite the valid concerns explored in chapter three, and due to the but-for effect, IP-based site blocking can be relied on as a faulty, yet sufficiently effective, mode of the tier 4 response, with the potential development of blocking technology being kept in mind as a potentially encouraging factor.

[1196] See section 3.1.1 of chapter four.
[1197] Belgian Supreme Court's decision taken on the 22nd October 2013, P.13.0550.N/1, available (in Flemish) at http://www.ipnews.be/wp-content/uploads/2013/11/20131022-Cassation-Telenet-The-Pirate-Bay.pdf
[1198] Poort et al, supra fn. 682.
[1199] Angelopoulos, supra fn. 933, at 820.

As O'Sullivan wrote in the context of copyright-based website blocking injunctions, "(w)hereas the Court of The Hague asserts that this endeavour is pointless where pirates find alternative sources, the fact remains that a denial of access has been achieved. In a deterrence strategy, denial has a twofold benefit: (1) it is reasonable to assume denial has a negative effect on piracy, and (2) it creates transaction costs for pirates and the operators of such websites".[1200]

In order to discuss the impact of access blocking within the specified request system on the human rights environment, it is worth referring to the ECtHR decision in *Ahmet Yildirim v Turkey* (2012),[1201] and more specifically, to the separate, concurring opinion of judge Pinto de Albuquerque, who attempted to provide guidance with regards to the Convention-compatible website blocking legislation. While the said guidance originates from the ECtHR, not the CJEU, it is argued that the specified request reform of EU law could use such guidance as an indication of how the discussed access blocking scheme fits (or should be shaped to fit) the human rights regime of the CFREU. To this end, the following paragraphs refer to each of the eleven factors mentioned by the judge Pinto, which Convention-compatible website blocking legislation should, in his opinion, endorse:[1202]

- (1) "a definition of the categories of persons and institutions liable to have their publications blocked, such as national or foreign owners of illegal content, websites or platforms, users of these sites or platforms and persons providing hyperlinks to illegal sites or platforms which have endorsed them" – The fourth tier of response access blocking system (referred to in this section as the SR blocking system) would indicate here the targeted platform' operators , the indexing services wishing to index it, as well as the platform's users, both those who are connected to infringing activities, as well as those who are not.
- (2) "a definition of the categories of blocking orders, such as blocking of

[1200] O'Sullivan, supra fn. 712, at 580.
[1201] *Ahmet Yildirim v Turkey* (2012) ECtHR, application no. 3111/10.
[1202] *Ahmet Yildirim v Turkey*, supra fn. 1201, at 27.

entire websites, Internet Protocol (IP) addresses, ports, network protocols or types of use, like social networking" – As mentioned above, the blockade would take place at the IP address level – and would be aimed at blocking the entire websites. The aim here is not to separate out and disable their sectors containing infringing content, it is to obtain their compliance with the specified request system – or put an end to their service's activity in cyberspace.

- (3) "a provision on the territorial ambit of the blocking order, which may have region-wide, nationwide, or even worldwide effect" – In the EU's model of specified request, which this chapter is focused on, the territorial ambit would be that of the European Union.
- (4) "a limit on the duration of the blocking order" – The blocking order would be limited in time to the moment in which the ISSP begins to comply with obligations ascribed to it, and evidence of this is presented to the suitable body of appeal.[1203]
- (5) "an indication of the "interests", in the sense of one or more of those included in Article 10 § 2 of the Convention, that may justify the blocking order" – Copyright, trademarks, privacy and reputation; all four match the criteria of art. 10(2), which refers to "the protection of the reputation or rights of others".
- (6) "observance of the criterion of proportionality, which provides for a fair balancing of freedom of expression and the competing "interests" pursued, while ensuring that the essence (or minimum core) of freedom of expression is respected" – This could be ensured by a combination of factors. Firstly, the blockade of a website on the fourth tier of response would be lifted as soon as the evidence of compliance would be presented – as described in point (4). Secondly, in the context at hand, the intermediary's freedom of expression[1204] should not outweigh the need to protect the interests mentioned in point (5), due to the time the ISSP would have to reply or comply during the first three tiers of response; the decision in *Neij* support this interpretation. As for the users of the website

[1203] A variant of which is presented in section 2.4.2 of this chapter.
[1204] As laid out in section 3.2.2 of chapter four.

and their access to legitimate content,[1205] they could be informed about the incoming blockade early enough to allow for backup (or deletion) of their content and transfer to a similar service of the same kind. Additionally, should the operator begin to comply, the website would become available again as a platform facilitating the exchange of legitimate information. While finding the adequate method for informing the users about the incoming blockade poses a challenge, it could be done by requiring this of the operator and/or maintaining a section on the website of the specified request agency, informing the public about the websites on the "last resort" tier of response. The final concern for the freedom of expression to be approached in this paragraph is tied to a situation in which a blocked IP address is shared by both the non-compliant and compliant (ie. legitimately operating) websites – an issue discussed in section 3.2.2 of chapter four. Husovec wrote after the *UPC Telekabel* decision that "website-blocking injunctions in all the Member States still must be strictly targeted. This means that any measures can only target those who infringed rights, whether as primary or secondary infringers. Any collateral over-blocking of innocent parties would render them disproportionate." According to Husovec, "the CJEU here confirms the principle of 'collateral censorship' first used by the European Court of Human Rights (ECtHR) in the *Ahmet Yıldırım v Turkey* case".[1206] Access blocking within the specified request should endorse this reasoning – however, the priority should be placed on the technological/infrastructural actions aimed at preventing the discussed sharing of IP addresses from taking place.

- (7) "compliance with the principle of necessity, which enables an assessment to be made as to whether the interference with freedom of expression adequately advances the "interests" pursued and goes no further than is necessary to meet the said 'social need' " – On the similar grounds as those listed in the previous point, the discussed blocking regime would pass this requirement. Furthermore, if after the first three tiers the ISSP still does not comply, the access blockade and the criminal

[1205] See section 3.2.1 of chapter four.
[1206] Husovec, supra fn. 1044, at 633. The principle in question was part of the dicta in the *Yildirim* case.

shutdown are the adequate, necessary steps – the former one being practically the only feasible route where non-EU intermediaries are considered. The specified request needs to contain a mode of response to the most notorious ISSP, and tier four access blocking provides a crucial part of it.

- (8) "definition of the authorities competent to issue a reasoned blocking order" – This would be a dedicated limb/tribunal of the specified request agency.
- (9) "a procedure to be followed for the issuance of that order, which includes the examination by the competent authority of the case file supporting the request for a blocking order and the hearing of evidence from the affected person or institution, unless this is impossible or incompatible with the "interests" pursued". – The "competent authority" would be the one from point (8) and it would offer the chance to reply and present evidence along each step of the compliance-inducing path.
- (10) "notification of the blocking order and the grounds for it to the person or institution affected" – As this is the final tier of response (with the ISSP being made aware of all tiers of response which await the lack of compliance), this requirement is filled with a surplus. Certainly, the ISSP would be informed that he is about to face the last resort measures.
- (11) "a judicial appeal procedure against the blocking order" – As it was mentioned in point (6), the blocking order is to be lifted if proof of compliance is shown, in front of the judicial limb of the specified request agency.

In addition to the effectiveness and human rights aspects of the discussed blocking mechanism, it is worth adding that further research should be conducted with regards to the exact technology which should be endorsed by the EU's ISPs. Such research should be continuous in nature, in order to get ahead and stay ahead of the rather likely circumvention efforts; and it should take into account the point at which the choice/implementation of the blocking technology should be left to the relevant intermediaries. The starting point for this analysis could be a thorough assessment of the Cleanfeed system used in

the *Newzbin2* injunctions.[1207] In any case, following the specified request logic, the ISPs' obligations within the tier four access blocking procedure should be as clear as possible.

2.3.2.4.2. Last resort response - criminal shutdowns.

Implementing the access blocking regime presented in the previous section would, without doubt, be a challenging endeavour, requiring prolonged negotiations between the Member States. This would be even more of a case for the second aspect of the fourth tier of a compliance response, based on criminal shutdowns – it would probably require a new, EU-wide offence, integrated with the specified request system. While the discussion concerning the latter's implementation is in section 2.4 of the current chapter, it already has to be mentioned that section 2.3 operates under the assumption that in the long-term, it *would be* possible to adapt the legal and institutional framework of the EU to accommodate the fourth tier of response as laid out. There is no doubt that the creation of a new, EU-wide offence is an immense and challenging task in itself. With this being cleared out, the following paragraphs can attempt to offer a few points of guidance with regards to how the criminal shutdowns at hand could be designed.

First of all, the target(s) of effective shutdowns has to be chosen – whether the police should go after the website's operators, servers and/or the domain name. Despite the weaknesses of each option, it is advised to rely on all three of them simultaneously. Arresting the operators may be insufficient for the closure of the targeted website or prevention of its revival, as the prosecutors in The Pirate Bay trial[1208] or *R v Rock and Overton*[1209] discovered. Seizing the servers on which the infringing website is hosted might be difficult if the hosting provider is located outside of the EU, and moreover, the operators

[1207] Discussed in section 2.3 of chapter three.
[1208] TPB trial, supra fn. 111.
[1209] *R v Rock and Overton*, supra fn. 90.

might have backup servers or switch to a new hosting provider; this line of concern being raised by Lodder and Meulen, as well as Lauinger et al above.[1210] Seizing the domain name leaves the website accessible through the IP address, and a new domain name can be obtained from a different registrar. Nevertheless, those three aspects complement each other and are not devoid of evidence supporting their flawed, yet visible effectiveness. On multiple occasions, the arrests did cause the targeted website to shut down – this being the case, for example, in the Megaupload crackdown. Moreover, the former proceedings produced evidence of a moderate deterrence effect, including intermediaries going into a no-sharing mode, banning connections from an area (here, this would be the EU) and closing elements of their service which encourage infringements (for example, the affiliate programs). Server seizures also produced results, in disabling websites such as TV Links or Oink's Pink Palace.[1211] Furthermore, according to the UKIPO report, BREIN agency's activities, including server seizures, led to the situation in which "the larger scale websites that enable access to unlawful content have fled Dutch jurisdiction and moved to other countries".[1212] Finally, while seizing the domain name is probably the weakest of all three measures, it still disrupts the website's operation and takes from the operators a possession of certain value.

Nonetheless, the diminishing returns perspective (discussed in section 4 of chapter three) has to be considered. Should empirical research indicate that the criminal shutdowns of websites on the fourth tier of response are significantly inefficient, this tier should be limited to the access blockade laid out in section 2.3.2.4.1 of the current chapter, for it is likely to remain on the satisfactory side of the point of diminishing returns.

Regarding the human rights dimension, two points can be made. Firstly, the freedom of expression-related risks tied to the removal of access to a website

[1210] See section 2.3 of chapter three.
[1211] As shown in section 3.2.1 of chapter two.
[1212] *International Comparison of Approaches to Online Copyright Infringement*, supra fn. 703, at 66. This, of course, shifts the line of enforcement back towards the blocking measures discussed in section 2.3.2.4.1 of the current chapter.

are proportional, in a similar manner to those tied to the website blocking mechanism outlined in the previous section. Secondly, in order to further mitigate the problem of users not being able to access their legitimate information (which occurred during, for example, the Megaupload shutdown), the police should explore the option of operating the targeted website for a set period of time after the seizure of servers, with the minimal infrastructure necessary for users to withdraw their content.

Finally, it is worth noting that the "mere prosecution" strategy (if it is to be seen as a strategy) from the Filesoup proceedings,[1213] which arguably goes against the rule of law and the presumption of innocence, does not have the space to develop within the fourth tier response, for in order to get to it, the first three have to fail first. There is no option to base the enforcement process on bringing in criminal charges and withdrawing them.

2.3.2.5. Monitoring the compliance procedures.

There is little doubt that, while the proposed set of compliance-inducing steps is a result of a fair amount of analysis, they should be extremely carefully monitored before and after their potential implementation, from both the effectiveness and human rights impact angles (as should the preliminary requirements). To provide an example justifying such a need – certain malicious operators could try to ignore their legitimising requirements until the third tier of compliance measures is applied to them, and then reactivate their service under a different name, company, hosting location etc. In such a case, steps should be taken to penalise such individuals directly, instead of playing the whack-a-mole game with their consequent ISSP incarnations. Moreover, the landscape of online infringements should be perpetually surveyed for the developments tied to infringing practices changing or bypassing the role of intermediaries – such as the drive towards decentralised

[1213] See section 3.2 of chapter three.

P2P filesharing, or sharing of content via mobile applications such as Popcorn Time.[1214]

2.4. Implementing the specified request approach within the EU.

Adopting the specified request approach within the European Union would be, without doubt, a long-term, resource-intensive endeavour, likely to require extended discussions and negotiations, on both Community and national levels. The aim of this final section is to discuss the major elements of this process and to provide answers to some of the dilemmas which would be likely to unfold on its path.

2.4.1. Implementation within the legal framework.

Each harmonising legal initiative on the European level has to take account of the principle of subsidiarity, set out in art. 5(3) of the Treaty on European Union. It states that "in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level". The specified request reform, aimed at providing a new, European-wide online enforcement regime aimed at infringing content online, a regime geared towards the improvements in effectiveness and human rights impact, would fulfil this criteria convincingly, especially given the transborder nature of Internet.

[1214] See http://www.pcworld.com/article/2973556/streaming-media/popcorn-time-users-are-now-getting-sued-by-the-movie-industry.html

With this preliminary matter discussed, the section can proceed to its projection of the implementation process of the specified request approach into the law of the EU. What is proposed is a two-tier approach. First tier would rely on the development of further Memoranda of Understanding (akin to the one on Counterfeit[1215]) enunciating the legitimising requirements outlined in section 2.3.1 of the current chapter. These agreements should expand beyond the offline counterfeit trade (to, for example, copyright, trademarks in general, privacy, defamation), and reach out towards the multiple categories of ISSPs which appeared throughout this work. And as a matter of fact, the EU Commission announced an intention to do exactly this, in the context of following the money flowing from the IP infringements. The action plan presented in 2014 provides that "the Commission will facilitate the development of further voluntary Memoranda of Understanding to reduce the profits of commercial scale IP infringements in the online environment, following Stakeholder Dialogues involving advertising service providers, payment services and shippers".[1216]

The second tier would take a step further and implement the fully unfolded, legally binding specified request system through a new EU directive, and a series of adjustments to existing EU laws. To start with the former: it would entail two principal provisions. The first would establish the institution responsible for operating the EU-wide specified request system, establish its competences (such as designing and updating the specified requests, as well as managing the compliance procedure described in section 2.3.2 of the current chapter) and clarify its relationship with the other bodies involved in the enforcement processes.

The second provision would create a new liability safe harbour, stating in essence that the ISSPs covered by this directive are not liable for the

[1215] Memorandum on counterfeit trade, supra fn. 1083.
[1216] *Towards a renewed consensus on the enforcement of Intellectual Property Rights: An EU Action Plan* (2014) Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions COM(2014) 392 final, at 6.

infringing actions of their users, as long as the former comply with the relevant legitimising requirements. In doing so, the directive would protect the compliant ISSPs from modes of intermediary liability such as those presented in section 3.1.1 of chapter two; namely the joint tort liability, the authorisation liability, liability for communication to the public, and publisher's liability. That being said, the safe harbour would not cover situations in which it is proven that the ISSP intended for the infringements to be committed or committed them itself. Additionally, the safe harbour provision should not become active before the full sets of legitimising and compliance-inducing requirements are agreed on and ready for implementation.

The legitimising requirements would not be laid out in the directive, in order to remain flexible towards the changing online environment; the case could be different for compliance requirements, which could be enclosed in the discussed instrument, but with an attached provision allowing for updates and amendments. Those requirements are less likely to require flexibility and more likely to require enshrinement in a legislative instrument, due to the potential severity of the response mechanisms, especially their fourth tier.

How would this directive's arrival affect the elements of the European legislative framework presented in chapter two? First of all, the new safe harbour provision (hereafter referred to as the SR safe harbour) would have to be reconciled with the existing liability limiting regime of arts. 12, 13 and 14 of the E-Commerce Directive (hereafter referred to as the ECD) – which, as it was argued in section 3.3 of the second chapter, is already bending and breaking. To start with the least problematic of the three, the art. 13 "caching" harbour; it seems that it could remain unchanged. Caching activities are not regulated in the proposed take on the specified request approach – and excluding liability for this technical procedure through art. 13 is quite sufficient. The situation with the "mere conduit" harbour of art. 12 is slightly more challenging. The specified request approach does not seek to dismantle the idea behind the protection of mere conduits. However, such protection

would also be granted by the SR safe harbour; and given the questionable use of art. 12 in cases such as *R v Rock Overton*[1217] or *R v Allan Ellis*[1218] (which involved torrent and filesharing sites, in contrast to, for example, *Bunt v Tilley*, which concerned ISPs, a group more suited to art. 12 protection) it could be reasonable to retire the "mere conduit" safe harbour.

While the conceptual background of the SR and art. 12 safe harbours was denoted as similar, the case with art. 14 of the ECD would be different. While it is also based on the premise of protection from liability conditional on the ISSP undertaking certain procedures (such as notice and takedown), the hosting harbour strips away the protection whenever actual or constructive knowledge of infringements is obtained by the ISSP. Such a line of reasoning has not proven logical or adequate in practice, leading to the problems such as the hosting intermediaries putting the "horse blinds" on and refraining from preventive monitoring measures. This line of concern is supported by the work of Friedmann[1219] and the findings of the report on the counterfeit Memorandum, which states that "(b)y taking proactive measures to prevent the sale of counterfeit goods, some Signatories were concerned that they could be held to have actual knowledge of the illegal activities that would put them outside the liability protection regime of the E-Commerce Directive".[1220] The specified request system does not seek to rely on such shaky criteria, which do not match its core principles. Hence, it is suggested that the discussed reform would have to include the removal of art. 14 of the ECD.

As for the provisions of the three E-Commerce Directive safe harbours reserving the right for the Member States' courts or administrative authorities to order a service provider to terminate or prevent infringements,[1221] they could be supported by an annotation providing that they apply, as long as the orders take account of/consider the specified requests tied to terminating or

[1217] *R v Rock Overton*, supra fn. 90.
[1218] *R v Allan Ellis*, supra fn. 113.
[1219] Friedmann, supra fn. 745, at 149.
[1220] Report on the memorandum on counterfeit, supra fn. 1082, at 11.
[1221] Described in section 3.3.1.1 of chapter two.

preventing infringements. Similar steps could also be undertaken with regards to the provisions of EU law warranting the use of intermediary-oriented injunctions, this including art. 8(3) of the InfoSoc Directive, arts. 9(1)(a) and 11 of the Enforcement Directive and art. 18 of the E-Commerce Directive. Recitals such as rec. 59 of the InfoSoc Directive, stating that the "conditions and modalities" of intermediary-oriented injunctions should be left entirely in the discretion of the national laws of the Member States, would also have to be reviewed.

While article 15 of the ECD does not directly contradict the core of the specified request approach, it would be advisable to either provide a more specific interpretation of its text (most notably of the term "general obligation"), or expand this article through legislative reform, as the corresponding guidance from the CJEU does not provide sufficient legal certainty. For example, as Husovec rightly notes, "(s)ome forms of website-blocking require all the attributes which *Sabam* and *Scarlet* seemed to outlaw in their cumulation. They are (i) exclusively implemented at the expense of a provider, use a filtering system of (ii) preventive nature for (iii) all electronic communications, which (iv) indiscriminately applies to all users and is issued for (v) unlimited period of time".[1222] In order to ensure the compatibility of multiple specified requests with art. 15 of the ECD, one of the two paths of reform proposed in the beginning of this paragraph should be endorsed.

An additional note should be made with regards to two notions, which should, to a large extent, accompany the process of implementing the specified request approach within the EU legal framework. The first one of them is transparency; it was highlighted by the EU Commission's report assessing the performance of the Memorandum on Counterfeit. This document proposes that "external transparency increases credibility and ensures accountability and responsibility towards stakeholders, national authorities and Parliaments as

[1222] Husovec, supra fn. 1044, at 634.

well as to society as a whole".[1223] An area as socially sensitive as the regulation of cyberspace fits extremely well within this statement. The second notion is that of cooperation with the stakeholders. Taking away the liability for users' infringements, and obliging the ISSPs to follow certain procedures in a certain way is an immensely delicate matter; getting it wrong could have severe consequences. Hence, it is unequivocally crucial to involve the ISSPs and other relevant stakeholders in the design of the specified request system, as well as in the progressive reviews of its performance.

2.4.2. Implementation within the institutional framework.

It is proposed that the agency supporting the implementation and operation of the specified request approach should be developed in two tiers – firstly, as an advisory body, obtaining required expertise and standing; and, secondly, as a regulatory body with powers and duties derived from the directive outlined in the previous section. Such duties would primarily be centred on designing and updating the legitimising requests, and operating the compliance procedure.

As for the institutional origin of the agency, there are two primary options. It would either be a new body, developed from the ground up and dedicated entirely to running the specified request system, or a body derived from one of the existing organisations. Examples of the latter could include the European Observatory on Infringements of Intellectual Property Rights (with its scope expanded beyond IP law) or one of the existing Directorates General of the EU Commission (from which a section focused on the specified request approach would be derived). On the one hand, the EU Commission's mandate, existing infrastructure and the need to reconcile its regulatory activity in the area of online enforcement with the functioning of the specified request system seem to make the latter option more appealing. On the other hand, the Observatory has a highly relevant, third party profile and it was actually

[1223] Report on the memorandum on counterfeit, supra fn. 1082, at 8.

identified in the Commission's report on the counterfeit Memorandum as an organisation which should assist non-signatories in adapting their practices to combat counterfeit: an activity matching those desired of the body in charge of the specified request system. While both options have certain merits, the author proposes for the Observatory to become the required institutional centre: a centre for cooperation between all stakeholders.

Bibliography

- **International agreements**
  - Convention on Cybercrime 2008.
  - WIPO Copyright Treaty 1996.
  - WIPO Performances and Phonograms Treaty 1996.
  - Agreement on Trade-Related Aspects of Intellectual Property Rights 1994.
  - International Covenant on Civil and Political Rights 1966.
  - International Covenant on Economic, Social and Cultural Rights 1966.
  - European Convention on Human Rights 1950.
  - Universal Declaration of Human Rights 1948.
  - Berne Convention 1886.
  - Paris Convention 1883.
- **Legislation**
  - ***EU***
    - Treaties
      - Treaty on the Functioning of the European Union
    - Regulations.
      - Council Regulation (EC) No 207/2009 of 26 February 2009 on the Community trade mark.
      - Council Regulation (EC) No 40/94 of 20 December 1993 on the Community trade mark.
    - Directives.
      - Directive 2008/95/EC of the European Parliament and of the Council of 22 October 2008 to approximate the laws of the Member States relating to trade marks.
      - Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related

to copyright in the field of intellectual property

- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
- Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.
- Directive 2002/58 of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
- 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 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 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services.
- Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector
- Directive 96/9/EC of the European Parliament and

of the Council of 11 March 1996 on the legal protection of databases

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs.
- Directive 89/104/EEC of 21 December 1988 to approximate the laws of the Member States relating to trade marks.

▪ Other.

- The Charter of Fundamental Rights of the European Union (2000/C 364/01).

○ ***UK***

▪ Deregulation Act 2015 c.56.
▪ Defamation Act 2013 c.26.
▪ Digital Economy Act 2010 c. 24.
▪ Serious Crime Act 2007 c. 27.
▪ Electronic Commerce (EC Directive) Regulations 2002.
▪ Human Rights Act 1998 c. 42.
▪ Data Protection Act 1998 c. 29.
▪ Defamation Act 1996 c. 31.
▪ Trade Marks Act 1994 c. 26.
▪ Broadcasting Act 1990 c. 42.
▪ Copyright, Designs and Patents Act 1988 c. 48.
▪ Senior Courts Act 1981 c. 54.

○ ***Other***

▪ France

- Loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet (HADOPI Law).

- US
    - Digital Millennium Copyright Act 1998.
    - United States Code.

- ***Germany***
    - Gesetz über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz) (geändert am 17. Dezember 2008) [Law on Copyright and Related Rights (as amended December 17, 2008)].

- ***Spain***
    - Ley 22/1987, de 11 de noviembre, de Propiedad Intelectual (Spanish Copyright Act).

- ***Proposed.***
    - Anti-Counterfeiting Trade Agreement 2012 (draft).
    - Proposal of the General Data Protection Regulation 2012/0011.
    - The Defamation Bill 2012-2013.
    - Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011.
    - Proposal for a European Parliament and Council Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights, COM (2005) 276/1

- **Case Law.**
    - ***CJEU***
        - Case C-348/13 *BestWater International GmbH v Michael Mebes and Stefan Potsch* [2014].
        - Case C-466/12 *Svensson v Retriever Sverige AB* [2014].
        - Case C-314/12 *UPC Telekabel v Constantin Film* [2014].
        - Case C-131/12 *Google Spain v Gonzalez* [2014].
        - Case C-293/12 *Digital Rights Ireland Ltd v Seitlinger* [2014].
        - Case C-360/10 *Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) v Netlog NV* [2012].
        - Case C-162/10 *Phonographic Performance (Ireland)*

Limited v Ireland and the Attorney General [2012].

- Case C-283/10 *Circ & Variete Globus Bucureşti v Uniunea Compozitorilor şi Muzicologilor din România - Asociaţia pentru Drepturi de Autor - U.C.M.R. - A.D.A* [2011].
- Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011].
- Case C-324/09 *L'Oréal SA v eBay International AG* [2011].
- Case C-393/09 *Bezpecnostni Softwarova Asociace - Svaz Softwarove Ochrany v Ministerstvo Kultury* [2010].
- Case C-569/08 *Internetportal und Marketing GmbH v Schlicht* [2010].
- Case C-236/08 *Google France SARL v Louis Vuitton Malletier SA* [2010].
- Case C-5/08 *Infopaq International A/S v Danske Dagblades Forening* [2009] ECDR 16.
- Case C-275/06 *Promusicae v Telefonica* [2008].
- Case C-306/05 *Sociedad General de Autores y Editores de Espana (SGAE) v Rafael Hoteles SL* [2006].
- Case C-176/03 *Commission v Council* [2005].
- Case C-101/01 *Bodil Lindqvist* [2003].
- ***
- Opinion of the Advocate General Cruz Villalón in the Case C-314/12.
- Opinion of the Advocate General Jaaskinen in Case C-131/12 *Google v Gonzalez*.
- Opinion of the Advocate General Cruz Villalón in the Case C-70/10.

- ***ECtHR***
  - The Grand Chamber ruling in *Delfi AS v Estonia* (2015), application no. 64569/09.
  - *Delfi AS v Estonia* (2013) ECtHR, application no. 64569/09.
  - *Neij and Sunde Kolmisoppi v Sweden* (2013) ECtHR, application no. 40397/12.

- *Ahmet Yildirim v Turkey* (2012) ECtHR, application no. 3111/10.
- *Kulis v Poland* (2009) ECtHR, application no. 27209/03.
- *Copland v UK* (2007) ECtHR, application no. 62617/00.
- *Hatton and Others v. the United Kingdom* (2003) ECtHR, 37 EHRR 28.

- ***UK***
  - *Cartier International AG v British Sky Broadcasting Ltd* [2014] EWHC 3354.
  - *The Football Association Premier League Ltd v British Sky Broadcasting Ltd & Others* [2013] EWHC 2058 (Ch).
  - *Paramount Home Entertainment International Ltd v British Sky Broad-casting Ltd* [2013] EWHC 3479 (Ch).
  - *Public Relations Consultants Association Ltd v Newspaper Licensing Agency Ltd* [2013] UKSC 18.
  - *EMI Records v British Sky Broadcasting* [2013] EWHC 379 (Ch).
  - *Tamiz v Google Inc* [2013] EWCA Civ 68.
  - *Tamiz v Google* [2012] EWHC 449 (QB).
  - *Golden Eye v Telefonica* [2012] EWHC 723 (Ch).
  - *Dramatico Entertainment v British Sky Broadcasting (No. 2)* [2012] EWHC 1152 (Ch).
  - *Twentieth Century Fox Film Corp v British Telecommunications plc* [2011] EWHC 1981 (Ch).
  - *CTB v News Group Newspapers* [2011] EWHC 1232 Q.B.
  - *Newspaper Licensing Agency Ltd v Meltwater Holding BV* [2011] EWCA Civ 890.
  - *Media CAT Ltd v. Adams* [2011] F.S.R. 29.
  - *Davison v Habeeb and others* [2011] EWHC 3031 (QB).
  - *ITV Broadcasting Ltd v TV Catchup Ltd* [2011] EWHC 1874 (Pat).
  - *CTB v News Group Newspapers* [2011] EWHC 1232 Q.B.
  - *CTB v. Twitter Inc., Persons Unknown* (2011) Queens Bench Division, HQ11X01814.)

- *Twentieth Century Fox Film Corp v Newzbin Ltd* [2010] EWHC 608 (Ch).
- *Kaschke v Gray* [2010] EWHC 690 (QB).
- *Joseph v Spiller* [2010] UKSC 53.
- *Scopelight Ltd v Chief Constable of Northumbria* [2010] Q. B. 438.
- *R. v Allan Ellis* T20087573 (2010) (at Middlesborough Crown Court).
- *R. v Rock and Overton* (2010) T20087573 (at Gloucester Crown Court).
- *l'Oréal v eBay* [2009] EWHC 1094 (Ch).
- *In re British Broadcasting Corporation* [2009] UKHL 34.
- *Metropolitan International Schools Ltd v Designtechnica* Corp (2009) EWHC 1765 Q.B.
- *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB).
- *Applause Store v Raphael* [2008] EWHC 1781 (QB).
- *Smith v ADVFN* [2008] EWHC 1797.
- *Bunt v Tilley* [2007] 1 WLR 1243.
- *Al-Amoudi v Brisard* [2007] 1 WLR 113
- *OBG Ltd v Allan* [2007] UKHL 21.
- *Sheffield Wednesday Football Club Ltd and Others v Hargreaves* [2007] EWHC 2375.
- *Galloway v Telegraph Group Ltd* [2006] EWCA Civ 17.
- *Lowe v Associated Newspapers Ltd* [2006] EWHC 320 (QB).
- *Jameel v Dow Jones & Co Inc* [2005] QB 946.
- *Polydor v Brown* [2005] EWHC 3191 (Ch).
- *Douglas v Hello! (No. 6)* [2005] EWCA Civ 595.
- *Reed Executive Plc v Reed Business Information Ltd* [2004] EWCA Civ 159.
- *Campbell v MGN Ltd* [2004] 2 A.C. 457.
- *Wainwright v Home Office* [2003] UKHL 53.
- *Re S* [2004] UKHL 47.

- *Sabaf SpA v MFI Furniture Centres Ltd* [2003] R.P.C. 14.
- *Chase v News Group Newspapers Ltd* [2002] EWCA Civ 1772.
- *Ashdown v Telegraph Group Ltd* [2001] EWCA Civ 1142.
- *Godfrey v Demon Internet Ltd* [2001] Q.B. 201.
- *Totalise v Motley Fool Ltd* [2001] EWCA Civ 1897.
- *Reynolds v Times Newspapers Ltd* [1999] 3 W.L.R. 1010.
- *R v Brown* [1996] A.C. 543.
- *Telnikoff v Matusevitch* [1992] 2 AC 343.
- *Kaye v Robertson* [1991] F.S.R. 62.
- *Unilever v Gillette* [1989] R.P.C. 583
- *CBS Songs Ltd v Amstrad Consumer Electronics Plc* [1988] A.C. 1013.
- *CBS Inc. v. Ames Records & Tapes Ltd* [1981] 2 All E.R. 812.
- *Trapp v Mackie* [1979] 1 W.L.R. 377.
- *Norwich Pharmacal Co v Commissioners of Customs and Excise* [1974] A.C. 133.
- *Scott v Commissioner of Police of the Metropolis*[1974] A.C. 819.
- *London Artists v* Littler [1969] 2 Q.B. 375.
- *Kemsley v Foot* [1952] A.C. 345.
- *Sim v Stretch* [1936] 2 All ER 1237.
- *Yousoupoff v MGM Pictures Ltd* [1934] 50 T.L.R. 581.
- *Tolley vs JS Fry & Sons Ltd* [1931] A.C. 333.
- *Falcon v Famous Players Film Co* [1926] 2 K.B. 474.
- *Adam v Ward* [1917] A.C. 309.
- *Hunt v Star Newspaper Co Ltd* [1908] 2 KB 309.
- *Merivale v Carson* (1887) 20 Q.B.D. 275.
- *McPherson v Daniels* (1829) 10 B. & C. 263.

- ***Other***
  - US
    - *UMG Recordings v Escape Media Group* (2012) Inc. 37 Misc.3d 208, 948 N.Y.S.2d 881 N.Y.Sup.

- *Louis Vuitton v Akanoc Solutions* (2011) US CoA 9th Cir. 10-15909.
- *Sony BMG v Tenenbaum* (2011) Nos. 10-1883, 10-1947, 10-2052.
- *Viacom International v Youtube* (2010) 07 Civ. 2103 (LLS).
- *Lenz v Universal Music Corp.* (2008) 572 F. Supp. 2D 1150.
- *MGM Studios, Inc. v Grokster, Ltd.* (2005) 545 U.S. 913.
- *Griffiths v United States of America* [2005] FCAFC 34.
- *A&M Records, Inc. v Napster, Inc.* (2001) 239F.3d 1004, 9th Circuit.

▪ France

- *TF1 v Youtube LLC* (2012), Court of First Instance Paris, judgement delivered on the 29th of May 2012.
- *Flach Films v Google Video* (2008) Commercial Court of Paris, judgment delivered on the 20th of February 2008.
- *The Myspace case* (2007), Tribunal of Grand Instance Paris, judgment delivered on the 13th of July 2007.
- *Zadig Prods v Google Video* (2007) High Court of First Instance of Paris, judgment delivered on the 19th October 2007.

▪ Germany

- *GEMA v Rapidshare* (2013) Federal Court of Justice, I ZR 80/12.
- The *Vorschaubilder II* case [2011] Federal Court of Justice, LZR 140/10.
- *Tutsche v Google* [2010] Federal Court of Justice, I ZR 69/08.

- *Atari v Rapidshare* (2010) OLG Düsseldorf, I-20 U 59/10.
- The *Uploaded.to* case (2012) AG Munich, Az.1111 Cs 404 Js 44538/07.
- The *Retroshare* case (2012) LG Hamburg, 308 O 319/12.

- Spain
  - *Telecinco v Youtube LLC* (2010) 289/2010, at Commercial Court no.7 (Madrid)
- Netherlands
  - *Ziggo & XS4ALL v BREIN* (2012) Hague Court of Appeal, case 200105418-01. See http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHDHA:2014:88
  - The Pirate Bay blocking orders (2012) Judgements of the Rechtbank's Gravenhage from the 11th of January and the 10th of May 2012.
  - *Stichting Bescherming Rechten Entertainment Industrie Nederland (BREIN) v Ziggo BV* (2010) 19 July 2010, District Court of the Hague.
- Norway
  - *Nordic Records Norway AS v Telenor ASA* [2010] 9 February 2010, Borgarting Court of Appeal
- Denmark
  - *IFPI Danmark v Tele 2 A/S* (2006) 25 October 2006, Copenhagen City Court.
- Austria
  - *Constantin Film v UPC* (2011) 13 May 2011, Commercial Court of Austria.
- Belgium
  - *Copiepresse v Google Inc.* [2011] 2007/AR/1730, at the Brussels Court of Appeal, 9th Chamber.
- Sweden

- *Columbia Pictures Industries Inc v Portlane AB* (2010) 4 May 2010, Swedish Court of Appeal.
- Case B-13301-06, District Court of Stockholm, judgment delivered on the 17th of April 2009.

▪ WTO

- Dispute DS362 *China - Measures Affecting the Protection and Enforcement of Intellectual Property Rights* (2009).

- **Academic resources.**
  - **Literature**
    - Books.
      - Goldrein I, *Privacy Injunctions and the Media* (Hart 2012).
      - Lloyd I, *Information Technology Law* (OUP 2011).
      - MacQueen H and others, *Contemporary Issues in Intellectual Property Law* (OUP 2011).
      - Helfer L and Austin G, *Human Rights and Intellectual Property: Mapping the Global Interface* (2011).
      - Collins M, *The Law of Defamation and the Internet* (OUP 2010, 3rd ed.)
      - Rogers W, *Winfield and Jolowicz on Tort (Eighteenth Edition)* (Sweet and Maxwell, 2010).
      - Price D and others, *Defamation: Law, Procedure and Practice* (Sweet and Maxwell 2010).
      - J Boyle, *The Public Domain: Enclosing the Commons of the Mind* (2008).
      - Goldsmith J and Wu T, *Who Controls the Internet? Illusions of a Borderless World*, (OUP 2006)
      - Walter M and Von Lewinski S, *European Copyright Law: A Commentary* (OUP 2010).
      - Laddie H, Prescott P& Vitoria M, *The Modern Law of Copyright* (Butterworths 1980)

- Articles.
    - Urban JM, Karaganis J and Schofield, BL, Notice and Takedown in Everyday Practice (March 29, 2016) UC Berkeley Public Law Research Paper No. 2755628, available at SSRN: http://ssrn.com/abstract=2755628
    - Lynskey O, 'Control over Personal Data in a Digital Age: *Google Spain v AEPD and Mario Costeja Gonzalez*' (2015) 78(3) MLR 522–548
    - O'Sullivan K, 'Enforcing copyright online: internet service provider obligations and the European Charter of Human Rights' (2014) 36(9), at 581.
    - Watson S, Zizzo D, Fleming P 'Determinants and Welfare Implications of Unlawful File Sharing: A Scoping Review' (2014) CREATe Working Paper 2014/05, available at http://www.create.ac.uk/wp-content/uploads/2014/04/Working-Paper-2014-15.pdf
    - James S, 'Digesting Lush v Amazon and UPC Telekabel: are we asking too much of online intermediaries?' (2014) Ent. L.R. 2014, 25(5).
    - Savola P, 'Blocking injunctions and website operators' liability for copyright infringement for user-generated links' (2014) E.I.P.R. 2014, 36(5), 279-288.
    - Husovec M, 'CJEU allowed website-blocking injunctions with some reservations' (2014), Journal of Intellectual Property Law & Practice, 2014, Vol. 9, No. 8
    - Friedmann D, 'Sinking the safe harbour with the legal certainty of strict liability in sight' (2014) Journal of Intellectual Property Law & Practice 9(2), at 149.

- Adermon A and Liang C-Y ‘Piracy and Music Sales: The Effects of an Anti-Piracy Law” (2014) Journal of Economic Behavior & Organization (105), 90.
- Angelopoulos C, ‘Are blocking injunctions against ISPs allowed in Europe? Copyright enforcement in the post-Telekabel EU legal landscape’ (2014) Journal of Intellectual Property Law & Practice, Vol. 9, No. 10.
- Hornle J, ‘Google's algorithms, search results and relevancy under data protection law - whose data quality?’ (2014) Ent. L. R. 25(6), at 211.
- Ramalho A, ‘Copyright law-making in the EU: what lies under the ‘internal market’ mask?’ (2014) Journal of Intellectual Property Law & Practice, 2014, Vol. 9, No. 3, Tsoutanis A, ‘Privacy and piracy in cyberspace: justice for all’(2014) Journal of Intellectual Property Law & Practice 8(12).
- Mac Sitigh D ‘The fragmentation of intermediary liability in the UK’ (2013) Journal of Intellectual Property Law & Practice 8(7), 521.
- Meale D, ‘Premier League 1, Internet pirates 0: sports streaming website the latest to be blocked’ (2013) Journal of Intellectual Property Law & Practice 8(11), 821.
- Barabash I, 'Ancillary copyright for publishers: the end of search engines and news aggregators in Germany?' (2013) E.I.P.R. 35(5), 243.
- Poort J, Leenheer J, Van Der Ham J, Dumitru C ‘Baywatch: two Approaches to Measure the Effects of Blocking Access to The Pirate Bay’ (2013), available at http://ssrn.com/abstract=2314297
- Gonzalez L, ‘Habeo Facebook ergo sum? Issues

around privacy and the right to be forgotten and the freedom of expression on online social networks' (2013) Ent. L.R. 83

- McEvedy L, 'Defamation and intermediaries: ISP defences' (2013) C.T.L.R. 2013, 19(4), at 108.
- Jones J, 'Internet pirates walk the plank with article 10 kept at bay: Neij and Sunde Kolmisoppi v Sweden' (2013) E.I.P.R. 35(11), at 697.
- Lauinger T and others, 'Clickonomics: Determining the Effect of Anti-Piracy Measures for One-Click Hosting' (2013), available at http://tobias.lauinger.name/#publications
- Danaher B and Smith M,'Gone in 60 Seconds: The Impact of the Megaupload Shutdown on Movie Sales (2013) (available at SSRN: http://ssrn.com/abstract=2229349).
- Sanders A, 'Intellectual property liability of consumers, facilitators and intermediaries: Comparative Concepts', in Heath C and Sanders A (eds), Intellectual property liability of consumers, facilitators and intermediaries (2012).
- James S, 'Tightening the net: defamation reform and ISPs.' (2012) Ent. L.R. 23(7), 197.
- Khan S, 'The potential impact on host intermediaries of defamatory remarks posted following L'Oréal v eBay.' (2012) C.T.L.R. 18(7), 204.
- Van der Ham J, Rood H, Dumitru C, Koning R, Sijm N, De Laat C, *Review en Herhaling BREIN Steekproeven* (2012), available at https://staff.fnwi.uva.nl/j.j.vanderham/research/publications/dutchpirate.pdf
- Kuschewsky M, 'The right to be forgotten – the fog finally lifts' (2012) P. & D.P. 10.

- Collingwood L, ‘Privacy in Cyberworld: Why Lock the Gate After the Horse Has Bolted?’ (2012) European Journal for Law and Technology, Vol. 3, No. 1, at 4.
- Danaher B and others, 'The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France' (2012), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989240
- Geiger C, 'The Anti-Counterfeiting Trade Agreement and Criminal Enforcement of Intellectual Property: What Consequences for the European Union?', in Rosen J (ed), *IP Rights at the Crossroads of Trade* (Edward Elgar 2012).
- Bitton M, 'Rethinking the Anti-Counterfeiting Trade Agreement's Criminal Copyright Enforcement Measures' (2012) Journal of Criminal Law and Criminology 102 (1), 67.
- Urbas G, 'Copyright, crime and computers: new legislative frameworks for intellectual property rights enforcement.' (2012) J.I.C.L.T. 7(1), 11.
- Garstka K, 'The Amended Digital Economy Act 2010 as an Unsuccessful Attempt to Solve the Stand Alone Complex of Online Piracy' (2012) IIC 43(2), 158.
- Lodder A and Meulen N, ‘Discussion of the Dutch Pirate Bay Case Law and Introducing Principles on Directness, Effectiveness, Costs, Relevance and Time’ (2012) JIPITEC 4(2), 130.
- De Hert P and Kloza D, ‘Internet (access) as a new fundamental right. Inflating thecurrent rights framework?’ (2012) European Journal of Law and

Technology, Vol. 3. No. 3.

- Bonadio E, 'Trade marks in online marketplaces: the CJEU's stance in L'Oréal v eBay.' (2012) C.T.L.R. 18(2), 37.
- Lievens D, 'L'Oréal v. eBay - welcomed in France, resented in England.' (2012) IIC 43(1), 68.
- Llewelyn D, 'Intellectual property liability of consumers, facilitators and intermediaries: Concepts under Common Law', in Heath C and Sanders A (eds), Intellectual property liability of consumers, facilitators and intermediaries (2012).
- Kulk S and Zuiderveen F, 'Filtering for copyright enforcement in Europe after the Sabam cases' (2012) E.I.P.R. 34(11) 791.
- Senftleben M, 'An Uneasy Case for Notice and Takedown: Context-Specific Trademark Rights' (2012) available at http://ssrn.com/abstract=2025075
- Cusack N, 'Is the Digital Economy Act 2010 the most effective and proportionate way to reduce online piracy?' (2011) E.I.P.R. 33(9), 559.
- Lemley M, 'Is the Sky Falling on the Content Industries?' (2011) Journal of Telecommunications and High Technology Law 9(1), 125.
- Tumbridge J, 'A cunning Fox defeats the pirates: 20th Century Fox v Newzbin' (2011) E.I.P.R. 33(6), 401.
- Daly A, 'The legality of deep packet inspection' (2011) I.J.C.L.P. 14.
- Hon W and others, 'The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, Part 1' (2011) I.D.P.L. 1(4), 211.

- Adam A, 'What is "commercial scale"? A critical analysis of the WTO panel decision in WT/DS362/R' (2011) E.I.P.R. 33(6), 342.
- Davies P 'Accessory liability: protecting intellectual property rights' (2011) I.P.Q. 4, 390.
- Crocker S and others, *Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill* (2011) (available at http://www.circleid.com/pdf/PROTECT-IP-Technical-Whitepaper-Final.pdf).
- Schrijvers M, 'European Court rules on the position of eBay regarding sale of infringing products: L'Oréal v eBay.' (2011) 33(11), 723.
- Kaminski M, 'An Overview and the Evolution of the Anti-Counterfeiting Trade Agreement (ACTA)' (2011) 21 Alb. L.J. Sci. & Tech., 385.
- Chaitowitz A and others, 'Responding to online piracy: mapping the legal and policy boundaries' (2011) 20 CommLaw Conspectus 1.
- Farrand B, 'The Digital Economy Act : cause for celebration or cause for concern?' (2010) E.I.P.R. 32(10), 536.
- Koempel F, 'Digital Economy Bill (Legislative Comment)' (2010) C.T.L.R. 16(2), 39.
- Bennett T, 'Horizontality's new horizons - re-examining horizontal effect: privacy, defamation and the Human Rights Act: Part 1' (2010) Ent. L. R. 21(3), at 103.
- Eziefula N, 'Getting in on the Act - OfCom publishes draft code on Digital Economy Act initial obligations' (2010) Ent. L.R. 21(7), 253.
- Ramsey L, 'Brandjacking on Social Networks:

Trademark infringement by impersonation of markholders' (2010) Buffalo Law Review 58(4), 851.

- Brown A and Waelde C, 'A practical analysis of the human rights paradox in intellectual property law: Russian Roulette', in Grosheide W (ed) Intellectual Property and Human Rights: A Paradox (2010).
- NJ King and P Jessen, 'Profiling the mobile customer - privacy concerns when behavioural advertisers target mobile phones: Parts 1 and 2' (2010) Computer, Law & Security Review 26(5), 455 and 26(6), 595.
- Reed C, 'Online and Offline Equivalence: Aspiration and Achievement' (2010) International Journal of Law and Information Technology 18(3), 248.
- Curtin T, 'The Name Game: Cybersquatting and Trademark Infringement on Social Media Websites' (2010) Journal of Law and Policy 19(1), 353.
- Taylor M and Matteucci M, 'Cloud Computing' (2010) C.T.L.R. 16(2), 57.
- Reed C, 'Information "Ownership" in the Cloud' (2010) Queen Mary School of Law Legal Studies Research Paper No. 45/2010, available at (http://ssrn.com/abstract=1562461).
- Akester P, 'The Impact of Digital Rights Management on Freedom of Expression – the First Empirical Assessment' (2010) 1 International Review of Intellectual Property and Competition Law 31.
- Akester P, 'The new challenges of striking the right balance between copyright protection and access to knowledge, information and culture' (2010) E.I.P.R.

32(8), at 372.

- Ormerod D, '*Scopelight Ltd v Chief of Police for Northumbria and Federation against Copyright Theft Ltd*: retention of seized material' (2009) Crim. L. R. 10, 733-736, at 736.
- MacQueen HL, "Appropriate for the digital age'? Copyright and the Internet: 1. Scope of Copyright.' in Edwards L and Waelde C (eds), *Law and Internet* (Hart 2009), 183.
- MacQueen HL, 'Appropriate for the digital age'? Copyright and the Internet: 2. Exceptions and Licensing', in Edwards L and Waelde C (eds) *Law and the Internet*, 3rd ed. (Hart Publishing 2009).
- Svensson M and Larsson S, 'Social Norms and Intellectual Property. Online Norms and the European Legal Development' (2009) Research Report in Sociology of Law, Vol. 1, Lund University (available through SSRN at http://ssrn.com/abstract=1598288).
- Manner M and others, 'The Pirate Bay ruling – when the fun and games end.' (2009) Ent.L.R. 20(6), 197.
- Strowel A, 'Internet Piracy as a Wake-up Call for Copyright Law Makers – Is the "Graduated Response" a Good Reply?' (2009) 1 WIPO Journal 75.
- Blakeney M, 'International Proposals for the Criminal Enforcement of Intellectual Property Rights: International Concern with Counterfeiting and Piracy.' (2009) I.P.Q. 1, 1.
- Edwards L, 'Mandy and Me: Some Thoughts on the Digital Economy Bill' (2009) SCRIPTed 6(3), 535.
- Edwards L, 'The Fall and Rise of Intermediary

Liability Online' in Edwards L and Waelde C (eds), *Law and Internet* (Hart 2009), 47.

- Valgaeren E and Roland N, 'Youtube and social networking sites – new kids on the block?', in Strowel A and Triaille J-P (eds), Google et les nouveaux services en ligne (2008).
- Lysonski S and Durvasula S 'Digital piracy of MP3s: consumer and ethical predispositions' (2008) Journal of Consumer Marketing 25(3), 167.
- Hsu J, Shiue C 'Consumers' willingness to pay for non-pirated software' (2008) Journal of Business Ethics, 81(4).
- Ponte L, 'Coming Attractions: Opportunities and Challenges in Thwarting Global Movie Piracy' (2008) 45 AM. BUS. L.J. 331.
- Rauhofer J 'Privacy is dead, get over it! Information privacy and the dream of a risk-free society' (2008) Information & Communications Technology Law 17(3), 185.
- Ginsburg J, 'Whose tube? Liability risks and limitations of copyright-dependent technology entrepreneurs', in Strowel A and Triaille J-P (eds), Google et les nouveaux services en ligne (2008).
- Ingram J and Hinduja S, 'Neutralizing music piracy: an empirical examination' (2008) Deviant Behavior 29(4), 334.
- Schultz M, 'Copynorms: Copyright Law and Social Norms' in Yu P (ed) *Intellectual Property and Information Wealth* (Praeger 2007).
- Levin, A, Dato-on, M, & Manolis, C 'Deterring illegal downloading: The effects of threat appeals, past behavior, subjective norms, and attributions of harm.' (2007) Journal of Consumer Behaviour 6

(2/3).

- Hilty R and others, 'Statement of the Max Planck Institute for Intellectual Property, Competition and Tax Law on the Proposal for a Directive of the European Parliament and the Council on Criminal Measures Aimed at Ensuring the Enforcement of Intellectual Property Rights' (2006) IIC 37 (8), 970.
- Schultz M, 'Fear and Norms and Rock & Roll: What Jambands Can Teach Us About Persuading People to Obey Copyright Law' (2006) 21 BERKELEY TECH. L.J. 651
- Zentner A, "File sharing and international sales of copyrighted music: An empirical analysis with a panel of countries" (2005) Topics in Economic Analysis & Policy 5(1).
- Clayton R, 'Failures in a Hybrid Content Blocking System' (2005), available at http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf
- Liebowitz S, 'Will MP3 downloads annihilate the record industry? The evidence so far' (2004) in Libecap G (ed), *Intellectual Property and Entrepreneurship*.
- Moohr G, 'The Problematic Role of Criminal Law in Regulating Use of Information: The Case of the Economic Espionage Act' (2002) 80 N.C. L. REV. 853.
- Hardy I, 'Criminal Copyright Infringement' (2002) Wm. & Mary Bill Rts. J. 305
- Lessig L, 'Law of the horse: What cyberlaw might teach' (1999) 113 Harvard Law Review 501.
- Reidenberg J, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1998) 76 (3) Texas Law Review 553.

- Easterbrook F, 'Cyberspace and the Law of the Horse' (1996) U Chi Legal F 207.
- Tyler T, 'Compliance with Intellectual Property Laws: A Psychological Perspective' (1996) 29 N.Y.U. J. INT'L L. & POL. 219.
- Sykes M and Matza D, 'Techniques of Neutralization: A Theory of Delinquency' (1957) American Sociological Review 22(6), 664.

- **Reports etc.**
  - *International Comparison of Approaches to Online Copyright Infringement* (2015) UKIPO.
  - *Upgrading the Single Market: more opportunities for people and business* (2015) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2015) 550
  - Internet Governance Forum, *The Charter of Human Rights and Principles for the Internet* (2014) 3rd ed.
  - *How Google Fights Piracy* report (2013) by Google, available at https://docs.google.com/file/d/0BwxyRPFduTN2dVFqYml5UENUeUE/edit
  - *Report from the Commission to the European Parliament and the Council on the functioning of the Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet* (2013) EU Commission, COM(2013) 209 final.
  - *Digital Music Report: Expanding Choice. Going Global* (2012) by IFPI.
  - *HADOPI, 1.5 year after the launch* HADOPI Report (2012).
  - *Note d' information: Analyse de l'impact de la fermeture de MegaUpload :+25,7% d'audience pour les plateformes de Catch-Up TV et de VOD* (2012) by HADOPI, available at:

(http://www.hadopi.fr/sites/default/files/page/pdf/Note_Fermeture_Megaupload.pdf)

- Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce (2000/31/EC) (2012).
- *Digital Opportunity: A Review of Intellectual Property and Growth* (2011) by Ian Hargreaves.
- Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet (2011), available at http://ec.europa.eu/internal_market/iprenforcement/docs/memorandum_04052011_en.pdf
- *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (2011)Frank La Rue, available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf .
- *Technical report: An Estimate of Infringing Use of the Internet* Envisional (2011) available at: http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf.
- *Copycats? Digital Consumers in the Online Age* CIBER Report for SABIP (2009).
- *Digital Britain Report* (2009) by DCMS & BIS.
- *Participative Web: User Created Content* (2007) OECD report of the Working Party on the Information Economy, available at http://www.oecd.org/dataoecd/57/14/38393115.pdf.
- Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet, available at https://wcd.coe.int/ViewDoc.jsp?id=1207291 .
- *Gowers Review of Intellectual Property* (2006) by Andrew Gowers.
- Communication from the Commission to the Council, the

European Parliament, the Economic and Social Committee and the Committee of the Regions - *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime – eEurope* (2001) (COM(2000) 890 final).

- Barlow JP, *A Declaration of Independence of Cyberspace*, (1996).
- *Report of the Faulks Committee on Defamation* (1975) (Cmnd 5909).