Summary:

The aim of the thesis is to make a review of the current state of law regarding to liability of intermediary online service providers of illegal information they transmit or store. The review is made in European context based on EU law by positivistic approach. More specifically, the scope of the thesis is the recent interpretations of the provisions of section 4 of the eCommerce Directive.

Narrow interpretation of the special liability regime provided for by the eCommerce Directive has been avoided by the Court of Justice of the European Union (ECJ). Definitions provided for by Articles 12—14 of the directive should be flexible in order to be applicable in dynamic technological environment and promote technological advance.

In order to avoid unjust burdens to businesses of online service providers, the general monitoring ban, provided for by Article 15 of the eCommerce Directive and confirmed by the ECJ, should be considered absolute. Specific monitoring measures are not covered by the ban and therefore they may be imposed on service provider in accordance with principle of proportionality in specific cases. Balancing interests at stake is essential before imposing any injunction on an intermediary service provider’s business.

Revision of the provisions concerning the intermediary service providers’ special liability regime is needed since only very few providers of modern online services based on user-generated content may benefit from the regime.

Keywords: European law, electronic commerce, principle of proportionality, fundamental rights, information society services
I give a permission the thesis to be utilised in the Rovaniemi Court of Appeal X
I give a permission the thesis to be read in the Library X
I give a permission the thesis to be read in the Provincial Library of Lapland (only those concerning Lapland) __
Liability of Intermediary Service Providers in the EU

Review of current developments

Master’s Thesis
29.4.2013
Johanna Tuohino
Faculty of Law
University of Lapland
# Table of Contents

#### Bibliography

III

#### Abbreviations

XIII

1 Introduction

1

1.1 Scope and purpose of the thesis

1

1.2 Methodology and materials

3

1.3 Definitions

5

1.4 Outline of the thesis

6

2 Liability of intermediaries of illegal content transmitted or stored

6

2.1 Liability of mere conduit and caching service providers

9

2.2 Liability of hosting service provider

10

2.2.1 Neutrality requirement

11

2.2.2 Storage but no knowledge interpretation

13

2.2.2.1 Storage of information

13

2.2.2.2 Awareness of illegal content of activities

15

2.2.3 Diligent economic operator interpretation

18

2.3 Evaluation

20

3 Injunctions on service providers’ business

23

3.1 Injunctions to protect intellectual property rights

24

3.2 How to distinguish specific and general monitoring

25

3.3 How to distinguish illegal content?

26

3.3.1 Country of origin principle

27

3.3.2 Harmonisation of criminal law within the EU

30

3.4 Proportionality of injunction

32

3.4.1 Balancing fundamental rights

34

3.4.2 Restrictions of fundamental rights

36

3.5 Techniques and procedures

37

3.5.1 Filtering systems

37

3.5.2 Blocking

39

3.5.3 Other traffic management measures

41

3.5.4 Lack of feasibility of injunctions

41

3.6 Requirement of net neutrality policy

43

4 Notification procedures

45

4.1 NTD procedures within Member States

45
4.2 Harmonised procedure in the EU?

5 Liability of service provider providing peer-to-peer arrangements

5.1 Definition of P2P

5.2 Requirements stemming from principle of proportionality

5.3 Service provider – offender, abettor or mere intermediary?

5.3.1 Pirate Bay cases in Sweden and Finland

5.3.2 Service provider’s criminal liability in P2P arrangements

5.4 Applicability of the special liability regime to P2P arrangements

5.5 Evaluation

6 Conclusions

6.1 Definitions of intermediary services should be understood broadly

6.2 Injunctions imposed on service providers must be proportional

6.3 De lege ferenda, position of intermediary service providers requires revision

6.4 Openness of the Internet policy – how to steer a ship in a storm?
Bibliography

Literature

Abbott 2009

Akdeniz 2010

Alexy 2005

Bergkamp 2003

Craig—De Búrca 2011

De Beer—Clemmer 2009

Edwards 2009
Edwards 2000

Frabboni 2010

Hellner 2006

Husa 2001

Hyrynen 2007

Innanen—Saarimäki 2012

Julia-Barcelo 2000

Kajan 2002
Kiikeri 2012

Kroes 2010

Kuipers 2012

Kulk 2012

Laakso 1999

Laguna de Paz 2012

Lodder—Kaspersen 2002

Marsden 2009
Montero—Van Enis 2011

Mäntysaari 2003

Siniketo 2010

Smith 2007

Sorvari 2005

Stalla-Bourdillon 2010

Still 2002

Talus 2013
Trzaskowski 2005

Van den Bogaert—Cuyvers 2011

Van Eecke 2011

Walden 2010

Official sources

*The European Commission*


Roadmap concerning the N&A initiative version 2, modified in June 2012


Communication COM(2011) 222 final of *The open internet and net neutrality in Europe* from the Commission to the European Parliament, the Council, The Economic and Social Committee and the Committee of the Regions of 19 April 2011

*Digital Agenda of Europe* COM(2010) 245 final/2, given 26 August 2010

Commission *Declaration on Net Neutrality* 2009/C 308/02, 18 December 2009


Communication COM(96) 487 final from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on Illegal and harmful content on the Internet, 16 October 1996

European Union

EU Action Plan on combating terrorism, by 11 June 2004 as revised

The Council of Europe

Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights in regard with search engines, 4 April 2012

Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet, 21 September 2011
Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters, 26 March 2008

National authorities

Bill of the Finnish Government HE 235/2010 vp

Bill of the Finnish Government HE 194/2001 vp

Studies


Case law

Court of Justice of European Union

T-336/07 Telefónica and Telefónica de España v. Commission, 29 March 2012 (Telefónica v. Commission)

Case C-360/10 Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV, 16 February 2012 (SABAM v. Netlog)
Case C-70/10 Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), 24 November 2011 (Scarlet Extended v. SABAM)

Joined Cases C-509/09 & 161/10, eDate Advertising v. X and Olivier Martinez and Robert Martinez v. MGN Limited, 25 October 2011 (eDate Advertising)

Case C-324/09 L’Oréal SA, Lancôme parfums et beauté & Cie SNC, Laboratoire Garnier & Cie, L’Oréal (UK) Ltd v. eBay International AG, eBay Europe SARL, eBay (UK) Ltd, Stephen Patts, Tracy Ratchford, Marie Ormsby, James Clarke, Joanna Clarke, Glen Fox, Rukhsana Bi; 12 July 2011 (L’Oréal and others v. eBay)

Joined cases C-236/08 to C-238/08 Google France SARL and Google Inc. v. Louis Vuitton Malletier SA (C-236/08), Google France SARL v. Vaticum SA and Luteciel SARL (C-237/08) and Google France SARL v. Centre national de recherche en relations humaines (CNRRH) SARL and Others (C-238/08), 23 March 2010 (Google France and Google)

Case C-275/06 Productores de Música de España (Promusicae) v. Telefónica de España SAU, 29 January 2008 (Promusicae)

Case C-101/01 Sweden v. Bodil Lindqvist, 6 November 2003 (Lindqvist)

Case C-62/00 Marks & Spencer plc v. Commissioners of Customs & Excise, 11 July 2002 (Marks & Spencer)


Case C-152/84 Marshall v. Southampton and South-West Hampshire Area Health Authority, 26 February 1986 (Marshall)

Case C-283/81 CILFIT and others v. Ministry of Health, and Lanificio di Gavardospa v. Ministry of Health, 6 October 1982 (CILFIT)
Case C-41/74 Yvonne Van Duyn v. Home Office, 4 December 1974 (Van Duyn v. Home Office)

Case C-6/64 Flaminio Costa v. ENEL (Ente nazionale energia elettrica, impresa già della Edison Volta), 15 July 1964 (Costa v. ENEL)

**Opinions of Advocate Generals**

Opinion of Advocate General Pedro Cruz Villalón in C-70/10 Scarlet Extended v. SABAM, 14 April 2011

Opinion of Advocate General Jääskinen on C-324/09 L’Oréal and others v. eBay, 9 December 2010

Opinion of Advocate General Poiares Maduro in joined Cases C-236/08, C-237/08 and C-238/08 Google France and Google v. Louis Vuitton, 22 September 2009

**European Court of Human rights**

Neij and Sunde Kolmisoppi v. Sweden no. 40397/12, 19 February 2013

Ahmet Yıldırım v. Turkey no. 3111/10, 18 December 2012

Jokitaipale and others v. Finland no. 43349/05, 6 April 2010

Castells v. Spain no. 11798/85, 23 April 1992

**United States**


MGM v. Grokster 380 F.3d 1154, filed 19 August 2004

In re: Aimster Copyright Litigation 334 F.3d 643, decided 30 June 2003

**Nordic countries**

Helsingin hovioikeus 383, S 12/1850, 8 February 2013 (DNA)
KKO 2010:47, 30 June 2010 (*Finreactor*)

Svea hovrätt B 4041-09, 17 April 2009 (*The Pirate Bay*)

**Other sources**


www.bittorrent.com
# Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AG</td>
<td>Advocate General</td>
</tr>
<tr>
<td>DMCA</td>
<td>Digital Millenium Copyright Act (US)</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention on Human Rights</td>
</tr>
<tr>
<td>ECJ</td>
<td>Court of Justice of European Union</td>
</tr>
<tr>
<td>ECtHR</td>
<td>European Court of Human Rights</td>
</tr>
<tr>
<td>e.g.</td>
<td>Exempli gratia; for example</td>
</tr>
<tr>
<td>etc</td>
<td>Et cetera</td>
</tr>
<tr>
<td>EU</td>
<td>The European Union</td>
</tr>
<tr>
<td>i.e.</td>
<td>Id est; it is</td>
</tr>
<tr>
<td>IT</td>
<td>Information technology</td>
</tr>
<tr>
<td>N&amp;A</td>
<td>Notice and action</td>
</tr>
<tr>
<td>NTD</td>
<td>Notice and take down</td>
</tr>
<tr>
<td>P2P</td>
<td>Peer-to-peer</td>
</tr>
<tr>
<td>TFEU</td>
<td>Treaty on the Functioning of the European Union</td>
</tr>
<tr>
<td>TEU</td>
<td>Treaty of the European Union</td>
</tr>
<tr>
<td>US</td>
<td>United States of America</td>
</tr>
</tbody>
</table>
1 Introduction to the subject matter

1.1 Scope and purpose of the thesis

In context of re-examination of the Directive 2000/31 (hereinafter eCommerce Directive) the European Commission (hereinafter Commission) has ceremoniously referred to “continuous process to ensure that Europe stays in the frontline of development and provides the best possible environment for e-commerce with a maximum level of legal certainty both for business and consumers whilst ensuring a minimum of burdens for business and Member States”.¹

It has become clear during the last two decades that the Internet provides plenty of benefits for businesses and individuals. The Internet economy has increased growth of economy at the national level² and provided for individuals opportunities to impart and receive information fast and at real time. While the Internet contributes freedom of expression, it makes it easy to breach as well. In the Internet and Web 2.0 era there is constant need for updated provisions and interpretations which are adapted to the reality of automatic data processing where lots of data, lawful and illegal, is generated by users with only a little control by side of the service provider. Moreover, the opportunity to share and download large amounts of data rapidly by using modern technology has made threshold to commit certain illegal activities lower, like unauthorised file-sharing and disseminating defamatory content. Users’ attitude has been noted to develop towards adoption of the new technology and the affirmation of new communication platforms³. These above-mentioned issues emphasize the constant need of online service providers, lawyers and national authorities for actual legal information of the area of law that is under pressure to adjust to the rapid development of technology.

Intermediary service providers are in crucial role in reaching the aims stated by the Commission as referred above. The aim of this thesis is to make a review of the current state of law regarding to liability of intermediary online service providers of illegal information they transmit or store. The review is made in European context based on EU law. More specifically, the scope of the thesis is the recent interpretations of the provisions of section 4 of the eCommerce Directive. These provisions concern liability of online service providers, to be exact the special liability regime provided for by Articles 12—14, and the prohibition to

³ See Frabboni 2010 p. 120.
set out general monitoring obligation on online service provider provided for by Article 15. In legal literature these provisions, called together as “dual ban”, have been considered being related to each other by promoting the same aims. The thesis makes a review of interpretations of the said provisions on a viewpoint of service providers. Therefore liability of individual recipients is not included to the scope of the thesis.

The Commission has acknowledged that “innovations and economic developments since the adoption of the [eCommerce] Directive in 2000 have rendered the interpretation of above-mentioned provisions increasingly challenging”. Reconciling of different interests concerning online liability has appeared to be anything but easy. This is why the thesis aims to clarify the role of intermediaries by reviewing applicability of the special liability regime and the coverage of the general monitoring ban in the current circumstances. With regard to these provisions, some of the most significant issues occurred in the market concern definition of ‘hosting service’, scope of general monitoring ban and liability issues of peer-to-peer (hereinafter P2P) networks. The latter is one example of a technological innovation and form of Web 2.0 based service which has become common among ordinary consumers. Of many options, P2P arrangements are chosen to be subject for further review.

The field where online service providers operate is considered international regardless of the purpose of an online service provider’s business and where the activities are directed to. The focus is chosen to cover the common market of the EU based on the international nature of the Internet. The primary focus is put on EU law and completed by some other sources, like practices and approaches of the Member States and sources considered as sources of inspiration in EU law. Another reason for the chosen focus relates to doctrines of EU law, namely concepts of direct effect and supremacy, which are reviewed briefly below in section 1.2 concerning methodology of the thesis. At this background in order to ensure legal certainty, the position of intermediary service providers in the common market of the EU should be interpreted in compliance with the harmonised provisions and in light of principles and doctrines of EU law. Telecom sector is subject to broad harmonisation in the EU which has been justified based on basic freedoms of the common market, namely freedom of establishment provided for by Article 49 TFEU and free movement of services provided for by Article 56 TFEU including free movement of information society services. At the above-

---

4 See Montero—Van Enis 2011 p. 27.
6 As an exception to this there are available some technological solutions to direct online content only to certain location by e.g. IP blocking measures.
mentioned background, focusing merely on interpretations of national law in assessing activities of those operating on the Internet cannot be considered sufficient in civil cases. Usually in criminal cases the effect of regarding provisions is not as binding as in civil cases due to competence of the EU. Questions concerning the competence will be reviewed further in the thesis.

To sum up, the general scope of the thesis is to review tools set out by EU law to ensure legal certainty in electronic commerce business from intermediary service providers’ point of view. The research questions the thesis is aiming to respond are i) *how the liability of an intermediary online service provider should be assessed in the light of current rulings of the Court of Justice of the European Union* (hereinafter ECJ), ii) *what national authorities should take into account before issuing injunctions on online service providers*, iii) *how measures restricting open character of the Internet should be approached in order to find a balance between interests at stake* and iv) *what should be taken into account concerning intermediary service provider’s liability in assessment of P2P arrangements*.

### 1.2 Methodology and materials

The thesis reviews the law by positivistic approach. To be exact, the chosen method is modern systematic positivistic theory of European law which aims to review law in context of legal system of the EU.\(^7\) Interpretations of the thesis are mainly based on rulings of the ECJ and the basic principles of EU law stemming from the Treaties and other primary legislation of the EU. Such basic principles include the basic freedoms of the internal market and the fundamental rights standards of the EU.

Understanding the concept of preliminary ruling provided for by Article 267 TFEU is an essential premise for the thesis. The aim of preliminary ruling procedure is to harmonise interpretation and applying of EU law in the common market regardless of a Member State.\(^8\) The relationship between national courts is reference-based, not an appeal system, and therefore the ECJ cannot determine validity of national law directly. This is why the rulings of the ECJ are considered prior rulings for national courts. The ECJ may give a ruling concerning interpretation of EU law which is binding in the concerning case where the

---

\(^7\) About positivistic theory of EU law and systemising the EU legal system see Kiikeri 2012.

\(^8\) Talus 2013 p. 80.
national court referred the question, but also more generally among the Member States through concepts of direct effect and supremacy.\(^9\)

Doctrines of direct effect and supremacy have been developed based on the case law of the ECJ. In early judgment *Van Duyn* the ECJ confirmed that directives could in principle have direct effect\(^10\) and clarified this interpretation in *Marshall* by limiting direct effect on vertical relations\(^11\). Later in *Marks & Spencer* the ECJ has declared that individual can also rely directly on provisions of a directive which are correctly implemented into national law but which have not been applied correctly in practice\(^12\). Supremacy refers to doctrine originating from *Costa v. ENEL* judgment according to which EU law should be accorded supremacy over national law. Supremacy has been considered as excluding national law that is inconsistent with EU law even though the EU provision would not have horizontal direct effect in concerning case.\(^13\)

The thesis rests on an assumption that interpretation based on rulings of the ECJ improves legal certainty inside of the common market. That is why in the modern international online environment the role of the ECJ is emphasized. The interpretation of the ECJ is evolutionary taking into account EU law as a whole, the objectives and state of evolution at the date on which the provision in question is to be applied.\(^14\)

In addition to the ECJ rulings, materials cover relevant EU legislation, especially the eCommerce Directive and other directives related to the common telecom framework and intellectual property rights. These sources are completed by interpretations originating from legal studies in the regarding field as well as from international and national case law, including rulings of the European Court of Human Rights (hereinafter ECtHR) and national courts of the Member States. The materials include also some comparative reviews to the case law of US because of the fact that in US have been given several internationally noted decisions concerning the topic of this thesis. Most of the materials utilised are relatively recent because of the aim of the thesis is namely to gather review of current developments regarding interpretation of the relevant provisions to the topic of the thesis. Despite of

\(^10\) C-41/74 *Van Duyn v. Home Office* [1974].
\(^11\) C-152/84 *Marshall v. Southampton and South-West Hampshire Area Health Authority* [1986].
\(^12\) C-62/00 *Marks & Spencer plc v. Commissioners of Customs & Excise* [2002] paragraphs 22—28.\(^13\)
\(^13\) C-6/64 *Flaminio Costa v. ENEL* [1964] and Craig—De Búrca p. 257—260.
\(^14\) C-283/81 *CILFIT* [1982] paragraph 20.
reviewing certain national case law of the Member States, the thesis does not focus on reviewing national implementation of the referred directives or other EU law.

1.3 Definitions

The definition of ‘information society service’ is essential in the scope of the thesis. This thesis regards information society services in means of relevant directives of EU law. The eCommerce Directive covers all information society services and therefore providing online services refers to business including providing information society services. In this context ‘information society service’ is understood as defined in Article 1(2) of directive 98/34 as amended.15

The thesis reviews the position of intermediary online service providers whose assignment is to transmit or store information provided by a recipient. Therefore ‘online intermediary service provider’ and ‘service provider’ in this thesis refers, in most of the cases, to a service provider in intermediary role in relation to the information transmitted or stored. Intermediaries include various actors who offer access to networks and/or other services16. In this thesis relevant service providers include especially access providers and platform providers17. The eCommerce Directive restricts liability of intermediary service providers providing ‘mere conduit’, ‘caching’ and ‘hosting services’ as defined in Articles 12—14 of the directive. Definitions of these services, especially definition of hosting service in Article 14, are reviewed further in the thesis in the light of case law of the ECJ and recent legal studies in the concerning field.

For the sake of clarity, it should be noted that rules of section 4 of the eCommerce Directive are designated by the names which are commonly used in legal literature. Articles 12—14 altogether constitute the entity which is called ‘special liability regime’, ‘liability shield’ or ‘liability restriction’ in this thesis. ‘General monitoring ban’ refers to rule originating from Article 15. ‘Dual ban’ refers to the section 4 of the directive as whole.

The topic of the thesis is closely connected to international human rights. Therefore both expressions ‘human rights’ and ‘fundamental rights’ refers to human rights and freedoms in international context. The latter refers especially to EU provisions, namely to the Charter of Fundamental Rights of the European Union (hereinafter Charter).

---

15 Information society services are reviewed further in the beginning of chapter 2.
17 See Frabboni 2010 p. 122.
1.4 Outline of the thesis

So-called dual ban is reviewed in the chapters 2 and 3. The second chapter discusses the liability of intermediaries by reviewing coverage of the special liability regime of the eCommerce Directive. The third chapter focuses on monitoring injunctions by reviewing coverage of the general monitoring ban and proportionality of different types of injunctions. The chapter reviews few of the common practices and procedures in the concerning field. It should be noted that the presented list of practices is not exhaustive or complete. The same regards to review of illegal activities typically pursued via intermediary services.

Following chapters 4 and 5 complete two previous chapters by reviewing notice and take down procedures in the fourth chapter and liability issues of service providers in P2P arrangements in the fifth chapter. NTD procedures are reviewed separately because they regard both of the topics of the chapter 2 and 3 and deserve some further attention as one potential practice which may be used for solving a set of issues concerning intermediary liability. P2P arrangements are reviewed in the chapter 5 by giving examples of application of the provisions and principles reviewed in the thesis. The chapter makes a brief review of approach towards the question of service provider’s liability in certain Swedish and Finnish cases by taking into account some aspects relating criminal law without going very deep into the criminal law. Neither intellectual property law is in the center of attention. The chosen national case law is not reviewed as precedents but as examples of phrasing questions within the current topic by aiming to contribute understanding of the cases that have aroused wide attention and confusion. Throughout the thesis the focus remains on liability of intermediaries in the common market of electronic commerce of the EU.

2 Liability of intermediaries of illegal content transmitted or stored

Intermediary service providers have a significant role in information society. No-one can publish or distribute material on the Internet without the aid of an intermediary. Intermediaries are therefore often involved to making available illegal and harmful material regardless whether they were aware of that or not. Those who happen to be victims of the infringing material are usually willing to direct claims on the intermediary rather than to the original infringer because of practical and historical reasons. Firstly, in practice it is usually easier to trace an intermediary service provider than an individual content provider who is

---

acting unknown to the public. Secondly, in some jurisdictions, like in UK and US, classically any person who publishes or re-publishes the defamatory statement has been considered liable as the original maker of the statement.19

The role of intermediary service providers is essential in contributing rights and freedoms of individuals, namely freedom of expression and protection of personal data, in online environment. Moreover, online services provide opportunities, not just for individuals, but also for businesses to pursue various activities contributing their own as well as national economic growth.20 Recital 2 of the eCommerce Directive refers to significant employment opportunities that development of electronic commerce offers, and stimulating economic growth and investing in innovation by European companies. These social and economic aims are the general aims of the internal market of the EU provided for by Article 3(3) TEU. Because of these social and economic aims, it has been considered important to improve legal certainty by coordinating rules and avoid obstacles on conducting business in online environment by limiting liability of intermediary online service providers. Section 4 of the eCommerce Directive has been described as a compromise between the interests of providers of intermediary services and those of the content industry, like creators and holders of rights to software, music, video, film, etc.21 However, the special liability regime of the eCommerce Directive is not limited to alleged intellectual property right infringements but it is applicable horizontally, within the scope of the eCommerce Directive, to civil and, to certain extent, criminal cases concerning transmitting or storing alleged illegal content22.

Taking into account competence of the EU, the conditions under which liability is determined are prescribed by national law of the Member States. However, the national provisions concerning the liability restriction must comply with the provisions of the eCommerce Directive and other applicable EU legislation through direct effect and supremacy doctrines in the legal system of the EU. Section 4 of the eCommerce Directive provides for the restriction of liability for certain intermediary online service providers of illegal content which they transmit or store. The aim of the restriction is to contribute objectives of the eCommerce Directive stemming from the Treaties — proper functioning of the common market by ensuring the free movement of information society services between the Member States and

---

19 See I bid.
20 In context of Digital Agenda for Europe COM(2010) 245 final/2 the Commission has referred to maximising “the social and economic potential of ICT, most notably the internet, a vital medium of economic and societal activity: for doing business, working, playing, communicating and expressing ourselves freely”(p. 3).
22 About illegal content see section 3.3.
balancing the different interests at stake. To put it briefly, the idea behind the liability restriction is to prevent from the situation where intermediary service providers would monitor and censor enormous amount of online information in order to manage the risk of being liable for the illegal information transmitted or stored. Such a behavior of market players would breach essential fundamental rights in information society, namely freedom of expression protected by Article 10 of the European Convention on Human Rights (hereinafter ECHR) and Article 11 of the Charter, and free movement of information society services protected by Article 56 TFEU. Moreover, harmonisation of online intermediaries’ liability is considered eliminating legal uncertainty in the common market.

The eCommerce Directive is limited in its scope. The directive applies to information society services which are defined in the Directive 98/34 as amended and recital 17 of the eCommerce Directive as “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services”. ‘Provided for remuneration’ does not require that the service is paid by the recipient but the service should represent economic activity. Therefore costs of providing the service can be covered for example by advertisement. ‘At a distance’ requirement is completed in annex V of the Directive 98/48 by leaving out of the scope services that are “provided in the physical presence of the provider and the recipient, even if they involve the use of electronic devices means”. ‘By electronic means’ refers to broad and technology neutral definition. In other words, it is required “that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means”. ‘At the individual request of a recipient of services’ refers to that service is provided through the transmission of data on individual request. In general, information society services should be understood media-neutrally covering wide range of

23 Article 1(1) and recital 41 of the eCommerce Directive contributes free movement of services provided for by Article 56 TFEU and the principle of proportionality. See Montero—Van Enis 2011 p. 21.
24 See Montero—Van Enis 2011 p. 21—22; and Van Eecke 2011 p. 1455—1456.
25 “To eliminate the existing legal uncertainty and to bring coherence to the different approaches that are emerging at Member State level, the proposal establishes a “mere conduit” exemption and limits service provider’s liability for other “intermediary” activities.” Proposal COM(1998) 586 final of 18 November 1998 p. 4.
26 Pursuant to Article 1(1) of eCommerce Directive its aim is “to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States”.
28 Lodder—Kaspersen 2002 p. 71; and Kroes 2010 p. 3.
29 Article 1(2) of directive 98/34 as amended by 98/48.
30 I bid.
online-activities\textsuperscript{31}. Moreover, the directive excludes certain areas of law, such as the field of taxation and gambling activities\textsuperscript{32}. Directive does not aim to harmonise criminal laws\textsuperscript{33} and cannot as such have binding effect in criminal law cases concerning interpretation of criminal liability of intermediaries.

The special liability regime covers mere conduit, caching and hosting services\textsuperscript{34}. Pursuant to the eCommerce Directive mere conduit and caching services consist of transmission of information in a communication network provided by a recipient of the service or the provision of access to a communication network. Caching is defined further as automatic, intermediate and temporary storage of information, provided by a recipient, which is performed for the sole purpose of making more efficient the information’s onward transmission to other recipients of the service.\textsuperscript{35} Hosting service consists of storage of information provided by the recipient of the service\textsuperscript{36}.

\subsection*{2.1 Liability restriction of mere conduit and caching service providers}

According to Article 12(1) of the eCommerce Directive a provider of mere conduit service shall enjoy the liability restriction when a service provider i) does not initiative the transmission, ii) does not select the receiver of the transmission, and ii) does not select or modify the information contained in the transmission. Mere conduit service may include storage of information only for the period that it is necessary for the sole purpose of carrying out the transmission in the communication network.\textsuperscript{37} Mere conduit services are provided typically by network operators and access providers\textsuperscript{38}.

According to Article 13(1) requirements for a caching service provider’s liability restriction are following: i) the provider does not modify the information; ii) the provider complies with conditions on access to the information; iii) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry; iv) 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 v) the service provider removes or disables access to information after obtaining actual knowledge of the fact that

\footnotesize{\textsuperscript{31}See recital 18 of directive 98/34 as amended by 98/48.\textsuperscript{\textsuperscript{32}}See Article 1(5) of the eCommerce Directive.\textsuperscript{\textsuperscript{33}}Recital 8 of the eCommerce Directive.\textsuperscript{\textsuperscript{34}}Articles 12—14 of the eCommerce Directive.\textsuperscript{\textsuperscript{35}}Articles 12(1) and 13(1) of the eCommerce Directive.\textsuperscript{\textsuperscript{36}}Article 14(1) of the eCommerce Directive.\textsuperscript{\textsuperscript{37}}Article 12(2) of the eCommerce Directive.\textsuperscript{\textsuperscript{38}}Hyyrynen 2007 p. 17.}
the information at the 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.

In both mere conduit and caching the storage of information is temporal but when compared to the mere conduit services the storage in caching lasts longer period and the information is available also for others than the recipient\(^{39}\). In turn, the storage in caching is more temporary than in hosting.

In case of mere conduit and caching services applicability of the liability restriction presumes that the activity of intermediary service provider is of a mere technical, automatic and passive nature.\(^{40}\) The service providers are entitled to the liability restriction provided that they do not modify the information or interfere transmitting of the information\(^{41}\). Applicability of neutrality requirement on mere conduit and caching is confirmed by the ECJ in *Google France and Google*\(^{42}\).

There have not been such significant issues regarding liability of mere conduit or caching providers which would have been arisen in the public discussion\(^{43}\). According to Bergkamp the special liability regime of mere conduit providers protects rightly conductors against liability claims since exposing them for liability would probably not prevent from many infringements and it would seriously effect on free flow of information. He also notes that the liability regime provides right incentives on caching providers, in case they are free to remove or disable access to information.\(^{44}\) At this background, it is reasoned to focus on the position of hosting service providers in this thesis since interpretation of hosting restriction has, contrary to mere conduit and caching restrictions, appeared to cause some ambiguity between studies.

### 2.2 Liability restriction of hosting service provider

What comes to hosting services, the question of neutrality does not seem to be as clear as in the case of mere conduit and caching. According to Article 14(1) of the eCommerce Directive the liability restriction applies on a hosting service provider when “*the provider does not have*
actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent” or that the service provider, “upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information”. When compared for example to the editors of online journals it is apparent that the position of intermediaries is more neutral than theirs, but should the hosting service provider share the same level of neutrality with mere conduit or caching service providers in order to be covered by the special liability regime?

The recent case law of the ECJ provides some guidance for interpretation regarding hosting services:

In SABAM v. Netlog the ECJ considered social networking platform, such as Netlog, being a hosting service provider in the meaning of Article 14 of eCommerce Directive. In Google France and Google and L’Oréal and others v. eBay the ECJ stated that the service does not fall within the scope of liability restriction if the service provider “plays an active role of such a kind as to give it knowledge of, or control over” the data it stores or transmits. The conduct of intermediary service provider should therefore be “merely technical, automatic and passive” in accordance with recital 42 of the eCommerce Directive. By the latter, the ECJ referred to all the three types of intermediary services including hosting as well.

2.2.1 Neutrality requirement

As referred above, the ECJ has considered neutral character of a service provider in its interpretation as a condition for applicability of the liability restriction provided for by Article 14 of the eCommerce Directive. The ECJ based this interpretation on wording of recital 42 of the directive according to which the liability exemptions established by the directive cover activity that is of “a mere technical, automatic and passive nature”. Furthermore, the ECJ has emphasized that the neutrality requirement based on recital 42 presumes that service provider “has neither knowledge of nor control over the information which is transmitted or stored”. In Google France and Google Advocate General Maduro approached the question of

---

47 See I bid.
neutrality via aim of special liability regime to create a free and open public domain on the Internet. According to him general monitoring ban of Article 15 is a key to that aim and it should be considered as expression of a principle that service providers which seek to benefit from a liability exemption should remain neutral in respect to the information they carry or host.\footnote{Opinion of AG Maduro in joined Cases C-236/08, C-237/08 and C-238/08 Google France and Google v. Louis Vuitton paragraphs 142—143.}

This interpretation in the ECJ’s rulings and Advocate General Maduro’s opinion in Google France and Google, that has been called “neutrality principle”\footnote{See Walden 2010 p. 207—208.}, has not been accepted without reservations. In L’Oréal and others v. eBay Advocate General Jääskinen has in his opinion expressed his doubts regarding to this approach by suggesting that recital 42 would not concern hosting services provided for by Article 14 of the eCommerce Directive. According to Jääskinen recital 42 of the directive, which speaks of “exemptions”, would refer to the exemptions discussed in the following recital 43 which expressly concern only mere conduit and caching\footnote{Opinion of AG Jääskinen on C-324/09 L’Oréal and others v. eBay paragraph 141.}. The approach of Jääskinen seems to be reasonable taking into account that Article 14 itself does not include any actual neutrality requirement. Moreover, according to Jääskinen the interpretation expressed in Google France and Google would seriously endanger the objectives of the eCommerce Directive\footnote{Ibid paragraph 142. Pursuant to Article 1(1) of the eCommerce Directive the directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States.}. Applying neutrality principle in hosting services has been criticised among legal studies as well. Walden has considered Maduro’s interpretation as attempt to recast the requirements for hosting service restriction in a manner which “fundamentally breaks the careful balancing act achieved by legislators”. He grounds this critique on his claim that Maduro has erroneously interpreted neutrality of illegal content as neutrality in respect of location, a specified place in cyberspace, which differs from traditional concept of neutrality \textit{vis-à-vis} the illegal content.\footnote{Walden 2010 p. 209.} Van Eecke rejects neutrality principle based on “Good Samaritan” paradox according to which voluntary and well-intended measures of service provider in order to prevent making available harmful content would lead to exclusion from liability restriction\footnote{Van Eecke 2011 p. 1483 and De Beer—Clemmer 2009 p. 405.}. Broad interpretation of the special liability regime in more general means has been supported as well. According to Edwards the regime is “designed on the whole to benefit rather than
burden the service provider”. Smith supports broad interpretation of Article 14 in order to broaden the coverage of the article on those who, in general sense, store third party information including for example such service providers who have outsourced the technical hosting function.

2.2.2 Storage but no knowledge interpretation

According to Van Eecke the ECJ’s interpretation, which he calls “storage but no knowledge”, seems reasonable if the neutrality requirement is replaced by a “lack of knowledge” requirement. He clarifies the storage but no knowledge interpretation in context of Article 14 by following inquiry:

“(1) Does the service considered involve any storage of user data? If not, the protection shall not apply. (2) Does the provider gain knowledge / awareness of certain illegal information through the general design or operation of the service? If yes, the protection shall not apply. (3) Even when the answer to the previous question is negative: was the provider nevertheless specifically informed about, or did he detect himself, specific illegal information? If so, the protection shall not apply if the provider does not promptly remove or block such information.”

Based on above-mentioned, the factual basis for the applicability of Article 14 consists of i) storage of information and ii) lack of awareness. These requirements are reviewed in following subsections.

2.2.2.1 Storage of information

As referred before, a hosting service, as intended in the eCommerce Directive, consists of storage of information. The term ‘information’ should be understood in a broad sense. A ‘hosting service’ has been defined as “providing a server on which the provider rents space to

---

58 Van Eecke 2011 p. 1472. Walden approaches applicability of hosting service providers with a little different phrasing of a question. According to him the steps are following: “First, does the conduct of the provider attract potential liability, whether primary or secondary in nature? If so, does the substantive law governing that form of conduct contain limitations of liability that would protect intermediaries engaged in ‘hosting’? If not, then if the conditions detailed in article 14 are present, the intermediary has a further defence to any liability.” Walden 2010 p. 205.
users for content, such as a web page, which may incorporate many kinds of material”\(^{60}\). The content stored and the way of storing varies a lot between hosting providers. The stored content can be computer programs, text documents, graphics, audio or video data or any other information. The files may be stored different ways: the Internet protocol used in storing dictating the software needed to access it varies, host can operate as e.g. mail server or news server.\(^{61}\)

Wording ‘consists of’ in Article 14(1) of the eCommerce Directive has been considered ambiguous. *Walden* considers the question whether the service should consist wholly or partly of storing data as “a key definitional boundary issue”.\(^{62}\) The Van Eecke’s formula referred above suggests that “any storage of user data” would fulfill the storage requirement. In other words, according to him Article 14 does not require that service would “mainly” consist of data storage. This is in line with the interpretations of Advocate Generals *Maduro* and *Jääskinen*. In *Google France and Google* Advocate General *Maduro* considered featuring certain content, which is both provided by the recipients of the service and stored at their request, nominally fulfilling conditions of hosting\(^{63}\). According to Advocate General *Jääskinen* in *L’Oréal and others v. eBay* reserving the exemptions to certain business types would be unworkable especially because of the constant and almost unpredictable change in the concerning area\(^{64}\). Furthermore, it has been claimed that “in practice, only a few services that would deserve special protection consist entirely of storage activities”\(^{65}\). *Smith* shares the similar line by arguing against narrow interpretation of Article 14. He suggests that limiting protection provided by Article 14 to the act of storage would limit utility of the provision by providing “protection from liability for an act of infringement consisting of copying (since that is what occurs when a work is stored) but not for making available to the public, since it occurs only to when the material is made available to be served up to a user and not upon mere storage”\(^{66}\).

So far the definition of storage has not achieved as much attention in the ECJ rulings as the question of awareness level. The ECJ has not assessed particularly whether the service should


\(^{62}\) See Walden 2010 p. 204.

\(^{63}\) Opinion of AG Maduro in joined cases C-236/08, C-237/08 and C-238/08 *Google France and Google* paragraph 138.

\(^{64}\) See Van Eecke 2011 p. 1473; and opinion of AG Jääskinen on C-324/09 *L’Oréal and others v. eBay* paragraph 148.

\(^{65}\) Legal analysis of a Single Market for the Information Society: 1. Executive summary p. 27.

\(^{66}\) Smith 2007 p. 380—381.
consist mainly or wholly of storage in order to fall within the scope of Article 14. However, intermediary services defined in Articles 12—14 are all covered by the liability restriction. It would be significant limitation for the applicability of the special liability regime to consider only those services, which fit into a coverage of one single service regulated in section 4 of the eCommerce Directive, being covered by the regime. If the service consists of all three types of intermediary service instead single one, it seems logical to interpret such a service being under the coverage of the special liability regime since all such activities are covered. The situation gets more unclear if a single service consists of storage but also of other activities which are not covered by the special liability regime. Still, at this background the flexible approach which does not narrow an applicability of the concerning provisions is justifiable taking into account needs of developing technology and the aim to contribute free movement of information society services in the common market as provided for by Article 56 TFEU.

2.2.2.2 Awareness of illegal content of activities

In the light of wording of Article 14 of the eCommerce Directive, the hosting service provider’s awareness of illegal content or activities pursued by a recipient of the service may be obtained by two ways. Service provider may have actual knowledge or constructive knowledge. Constructive knowledge means that a service provider is aware of facts or circumstances from which the illegality is apparent. The directive does not give any further guidance of how actual knowledge should be determined. According to Edwards bright line of regime of the eCommerce Directive has been that an intermediary is not prima facie liable in respect of content supplied by, or activities of, third parties, unless it has knowledge or complicity. Taking into account recent case law of the ECJ, the evaluation seems not that simple anymore.

As it has been referred in the Commission’s proposal as well as in several commentaries, according to the directive actual knowledge of illegal information or activities constitutes basis for criminal liability while civil liability may be based on both, actual or constructive knowledge. Such an idea seems erroneous in respect of criminal liability taking into account competence of the EU. Firstly, the directive does not aim to harmonise criminal laws as such

---

67 Edwards 2009 p. 84.
of the Member States\textsuperscript{69} and it cannot to have such an effect that it would define the matters that criminal liability should be based on. In other words, the EU does not have competence to regulate material national criminal law since there is no such provision given pursuant to Articles 82 or 83 TFEU that would effect on substantive criminal law.

Apparently, the incompatibility of the interpretation which dominated just after the directive was enacted has been noted by the ECJ. It has not addressed itself to distinguish actual and constructive knowledge but it has approached the question of awareness by a little different angle. At first in the awareness interpretation, the ECJ has assessed whether the service provider “plays an active role such a kind as to give it knowledge of, or control over, the data stored”. According to the ECJ’s line of interpretation, if the service provider has not played such an active role, that service provider cannot be held liable for the data which it has stored at the request of a recipient based on the first criterion.\textsuperscript{70} According to Van Eecke this means that “the service provider should not obtain knowledge of what is stored on its systems by virtue of the general way in which its service is designed or operated”\textsuperscript{71}.

In \textit{Google France and Google} the ECJ stated that concordance between the keyword selected and the search term entered by an Internet user is not sufficient of itself to justify the view that Google has knowledge of, or control over, the data stored in its memory. Instead the drafting of the commercial message which accompanies the advertising link or in the establishment or selection of keywords was considered relevant.\textsuperscript{72}

In \textit{L’Oréal and others v. eBay} the ECJ considered that “the mere fact that the operator of an online marketplace stores offers for sale on its server, sets the terms of its service, is remunerated for that service and provides general information to its customers cannot have the effect of denying it the exemptions from liability provided for by Directive 2000/31”. However, the ECJ considered that providing assistance, “which entails optimising the presentation of the offers

\textsuperscript{69} Recital 8 of the eCommerce Directive.
\textsuperscript{70} Joined cases C-236/08, C-237/08 and C-238/08 Google France and Google v. Louis Vuitton [2010] paragraph 120; and C-324/09 L’Oréal and others v. eBay [2011] paragraph 123.
\textsuperscript{71} Van Eecke 2011 p. 1472.
\textsuperscript{72} Joined cases C-236/08, C-237/08 and C-238/08 Google France and Google v. Louis Vuitton [2010] paragraphs 117 and 118.
for sale in question or promoting those offers”, indicating an active role of the service provider.73

Another criterion set by the ECJ regards Article 14(1)(b). In case a service provider has not played such an active role as referred above, the provider can be held liable for the data which it has stored, if it has failed to expeditiously remove or disable access to the data after obtaining knowledge of the unlawful nature of the data or of that recipient’s activities.74 Moreover, the ECJ has considered knowledge requirement broadly. In L’Oréal and others v. eBay the ECJ has stated that conditions set out in Article 14 must be interpreted as “covering every situation in which the provider concerned becomes aware, in one way or another, of such facts or circumstances”. The ECJ clarified further that a service provider may become aware of illegal activities as a result of its own investigations, as well as by notification based on sufficiently precise or adequately substantiated information.75

Despite the guidance provided by the ECJ, the Member States have introduced diverging interpretations with regard to obtaining knowledge in the meaning of Article 14. Bergkamp considers it questionable whether the low threshold of civil liability based on constructive knowledge serves any useful purpose. According to him it may lead to many false-positive decisions to terminate hosting arrangements and liability judgment based on hindsight.76 One may consider such critique reasonable since actual and constructive knowledge may be, and are, interpreted in varying way in practice. For example, according to public consultation organised by the Commission there are three dominating interpretations regarding actual knowledge: 1) an intermediary can only obtain actual knowledge through a court order; 2) an intermediary can only obtain actual knowledge through a notice (ranging from an 'informal' notice from a user, such as a red flag under a video, to a court order); or 3) an intermediary can obtain knowledge even in the absence of a notice if it, for instance, has a “general awareness” that its site hosts illegal information.77

Based on the ECJ’s ruling, as referred above, the interpretation of Article 14 should cover own investigations of a service provider and all notices which are based on sufficient information. It is clear that a service provider cannot claim having lack of knowledge after a

74 Joined cases C-236/08, C-237/08 and C-238/08 Google France and Google v. Louis Vuitton [2010] paragraph 120.
75 C-324/09 L’Oréal and others v. eBay [2011] paragraphs 121 and 122.
76 Bergkamp 2003 p. 33.
formal notification, and in the light of the ECJ’s interpretation, neither after a well-founded informal notification. Edwards comes into conclusion that “a bright line of no liability on intermediaries for content provided by third party content providers, unless or until notice is given to take down, can no longer be sustained”\(^\text{78}\). However, general awareness as constituting actual knowledge seems to be quite complicated in practice. General awareness interpretation would be likely to effect on behavior of service providers via before-mentioned “Good Samaritan paradox” by causing avoidance of own investigations since it is unclear what behavior will constitute assumption of awareness based on an active role of a service provider.

To sum up, interpretation based on division into actual and constructive knowledge does not offer much of help for national courts. Instead, the ECJ’s ruling in *L’Oréal and others v. eBay* does. It clearly expands coverage of Article 14 to every situation in which an intermediary service provider becomes aware of illegal content or activity. It is therefore matter of national courts to figure out whether there is sufficient evidence of awareness. What comes to reducing legal uncertainty, service providers need to know the consequences of conducting voluntary activities as well as taking down the alleged illegal material but also the risks of staying passive. Moreover, service providers need to know how rapid actions are required, for example whether there is time for legal consultation. The ECJ has given some guidance of how behavior of service provider should be assessed by setting out “diligent economic operator” criterion which will be reviewed in the following section. In addition to this, the question of interpretation would likely be clarified if the Commission will succeed with its initiative given in 2012 of harmonised notice and action procedure\(^\text{79}\).

2.2.3 Diligent economic operator interpretation

In *L’Oréal and others v. eBay* the ECJ has estimated awareness of the service provider based on the circumstances in which “a diligent economic operator should have identified the illegality in question”\(^\text{80}\). Due to international character of the Internet, illegality of the activity or information may not be obvious *per se*. According to Van Eecke the ECJ imposed, by setting out a diligent economic operator criterion, a high threshold, because *any* diligent economic operator should identify the information being illegal\(^\text{81}\). Later on, the ECJ has made use of the diligent economic operator assessment in competition case *Telefónica v.*

\(^{78}\) Edwards 2009 p. 87.
\(^{79}\) See section 4.2.
\(^{80}\) See C-324/09 *L’Oréal and others v. eBay* [2011] paragraph 120.
\(^{81}\) See Van Eecke 2011 p. 1467. Italics writers.
*Commission* in which the ECJ defined a diligent economic operator as such which “ought to have been familiar with the principles governing market definition in competition cases and, where necessary, taken appropriate legal advice to assess, to a degree that is reasonable in the circumstances, the consequences that a given act may entail”

Based on the rulings of the ECJ, one may say that a diligent economic operator should be aware of basic principles and be prepared for typical risks with regard to the market. Moreover in context of diligent economic operator interpretation, the ECJ has evaluated that the assumption that a diligent economic operator should be aware of decisions of authorities and the Community not applicable to small undertakings. Since the referred case law regards to situations differing from the situations reviewed in this thesis these approaches are only suggestive. The diligence of operator must be reviewed by taking into account all the prevailing circumstances. However, would it be too much to require that a diligent economic operator should be aware of at least of those risks that have occurred in the respective market and which are under public discussion?

An intermediary service provider seems to be in contradictory situation. A service provider may not be willing to block or remove information stored on request of its customers because of legal uncertainty and economic reasons. The eCommerce directive does not include any shield for a service provider against claims of their users regarding taking down lawful material. In case the notification of illegal content is given formal way, service providers may not be pleased of “putting up blocks between them and their paying customers”. Moreover, service providers are expected to contribute fundamental rights of users and other people. Pursuant to recital 46 of the eCommerce Directive the removal or disabling of access performed by service provider “has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level”.

---

83 For example joined cases T-298/97, T-312/97, T-313/97, T-315/97, T-319/97, T-600/97-T-607/97, T-1/98, T-3/98-T-6/98 and T-23/98 Mauro Alzetta and others v. Commission concerning state aids the ECJ stated following “the case-law of the Court of Justice to the effect that a diligent economic operator must be in a position to ascertain that the procedure provided for by Article 93(3) of the Treaty has been observed is not applicable in this instance, because most of the recipients were small firms which cannot be criticised for not having a precise and comprehensive knowledge of the decisions of national and Community authorities concerning the aid in question”.
84 See Van Eecke 2011 p. 1467—1468.
85 Abbott reminds that file-hosting services are legitimate businesses and “they will not take kindly to anyone putting up blocks between them and their paying customers” (Abbott 2009 p. 6).
2.3 Evaluation

Evolutionary character of the ECJ’s interpretation becomes essential in online environment. Evolutionary character of the ECJ interpretation was taken into account in C-283/81 CILFIT [1982] paragraph 20, according to which: “Finally every provision of Community law must be placed in its own context and interpreted in the light of the provisions of Community law as a whole, regard being had to the objectives thereof and to its state of evolution at the date on which the provision in question is to be applied.”

During Web 2.0 era amount and popularity of services offering a platform for user-generated content have increased significantly. Because of this in general, broad interpretations of the reviewed provisions of the eCommerce Directive is justified in order to improve compatibility of provisions with modern evolving online services. Moreover, the market of information society services has developed rapidly after introducing the directive, and the directive seems to be behind of the changes. According to many legal studies narrow interpretation of Article 14 would decrease its utility and therefore hinder reaching the aims of the directive, namely free movement of information society services stemming from Article 56 TFEU. In general, the ECJ has leant on quite broad interpretation when considering definition of hosting service and obtaining awareness of illegal content. However, by extending coverage of neutrality principle to hosting services, as to mere conduit and caching services by virtue of recital 42 of the eCommerce Directive, the ECJ has narrowed interpretation of Article 14 the way which may be called into question. However, in the context of EU law it should be born on mind that the ECJ rulings are binding in respect to the interpretation of EU law by virtue of supremacy doctrine. At this point it is interesting to see how the ECJ’s interpretation will develop regarding neutrality principle and whether the ECJ will take into consideration the given critique.

The inquiry of Van Eecke, which was referred before, sets out fair basis in assessment of hosting services based on rulings of the ECJ. Taking into account remarks made in this chapter, the inquiry should be completed by few more questions. In order to assess applicability of the special liability regime of the eCommerce Directive the nature of the service provider’s economic activity must be reviewed at first. Therefore, the first question would be whether the services provided by the provider are information society services as defined in the Directive 98/34 as amended. If the answer is yes, the next question concerns the level of the service provider’s activity in relation to the online content stored. In case of mere conduit or caching services, contrary to hosting, it is justified to evaluate activity based on the

---

86 Evolutionary character of the ECJ interpretation was taken into account in C-283/81 CILFIT [1982] paragraph 20, according to which: “Finally every provision of Community law must be placed in its own context and interpreted in the light of the provisions of Community law as a whole, regard being had to the objectives thereof and to its state of evolution at the date on which the provision in question is to be applied.”


88 The supremacy doctrine was introduced in early ECJ ruling C-6/64 Flaminio Costa v. ENEL [1964]. See Craig—De Búrca p. 256—258.
referred neutrality principle by taking into consideration wording of Articles 12 and 13 of the eCommerce Directive.

If the service consists of storing data, wholly or partly, the restriction may apply based on Article 14. The neutrality principle as such seems not to be a sufficient ground for interpretation based on the wording of Article 14, the objectives of the eCommerce Directive and critique given by various legal studies. Applying the neutrality principle in hosting services would restrict applicability of the special liability regime notably and therefore it should be approached with carefulness. Instead of neutrality, the attention should be paid on an activeness of a service provider, in accordance with the relevant rulings of the ECJ, in order to assess the service provider’s awareness of the information stored. Therefore in case of a hosting service, which consists of storage of information, the relevant question is whether the service provider has got aware of the illegal content. Awareness can be tested by following questionnaire which is based on Van Eecke’s inquiry:

1) Does the service provider have an active role of such a kind as to give it knowledge of, or control over, the data it stores? If the answer is no, liability restriction may apply and the next question is following: 2) Does the service provider got aware of illegal activity or information otherwise for example by its own inspection, claims of damages or via any sufficiently precise or adequately substantiated notification? If the answer is no liability restriction applies. If the answer is yes to the previous question it should be found out 3) whether the service provider acted in accordance with Article 14(1)(b) of the eCommerce Directive and removed or disabled the information. If the answer is yes the liability restriction of hosting service provider applies.

The storing but no knowledge principle is completed by the ECJ’s diligent economic operator principle which applies in assessing the awareness of illegality. Diligent service provider is expected to know the basic risks in the field it operates and to be prepared for those risks to the certain point. Hosting services covers wide range of activities and are provided by service providers with varying capacity. Therefore, it is justified to review the diligence on case-by-case basis. The ECJ ruling in Telefónica v. Commission suggests that the diligent service providers are expected to assess consequences of their acts by taking legal advice when

---

89 See Van Eecke 2011 p. 1473; and section 2.2.2.
necessary. One may get to the conclusion that the ECJ expects a diligent economic operator to actively assess claims and notifications of illegal content or activity and consult a lawyer if needed. Because of that, it would be beneficial to implement the diligent economic operator principle to the risk management of an intermediary service provider. On the other hand, it should be born in mind that service providers should not be evoked to take such monitoring or censoring measures that would restrict open character of the Internet.

As referred before, balancing various interests is one of the aims of the eCommerce Directive. The idea behind the liability restriction is to promote freedom of expression whereas free movement of information society services can be considered as “a specific reflection” of freedom of expression. The other interests, like protection of personal data and intellectual property rights, must be taken into account as well. Still, freedom of expression seems to have a special role. According to Advocate General Maduro in Google France and Google the aim of the directive is to create “a free and open public domain on the internet” which can be considered as one reflection of freedom of expression as well. Nevertheless, freedom of expression has been considered as an essential part of the net neutrality policy of the EU. According to recommendation CM/Rec(2011)8 of the Committee of Ministers “the protection of freedom of expression and access to information on the Internet and the promotion of the public service value of the Internet are part of a larger set of concerns about how to ensure the universality, integrity and openness of the Internet”.

Against this background especially in the light of the objectives set out in the eCommerce Directive, one could claim that in balancing interests in interpretation of hosting provider’s liability a cut above other interests is freedom of expression. According to a little more cautious approach it would be well-founded to consider freedom of expression having, instead of prevalence, a special role in balancing interests. As referred before, the aim of the liability restriction is to avoid situation where an intermediary service provider is willing to implement restrictive censoring or monitoring measures in order manage with the risk of liability of the information they transmit or store provided by a recipient of service.

---

91 Recital 9 of the eCommerce Directive.
92 Opinion of AG Maduro in joined cases C-236/08, C-237/08 and C-238/08 Google France and Google v. Louis Vuitton paragraph 142.
93 Recommendation CM/Rec(2011)8 paragraph 7. According to the Commission Declaration on Net Neutrality 2009/C 308/02, given in relation to revision of common telecoms framework, net neutrality is considered as policy objective and regulatory principle of the common telecom framework.
94 About balancing of interests see section 3.4.1.
Not only service providers have interest to control contents in the online service. Service providers may be mandated pursuant national law by national authorities to take measures in order to prevent illegal activities. The next chapter reviews interpretation of the general monitoring ban provided for by Article 15 of the eCommerce Directive.

3 Injunctions on service providers’ business

Pursuant to Article 15(1) of the eCommerce Directive the Member States cannot set obligation on mere conduit, catching or hosting service providers to generally monitor the information they transmit or store. In addition to this, Article 15(1) prohibits national authorities from setting out general obligation on service providers to actively seek facts or circumstances indicating illegal activity. The ban of general monitoring has been justified by freedom of expression, avoiding preventive censorship and practical reasons. Moreover, the ban contributes the objective of the eCommerce Directive set out by recital 8 which is stemming from Article 56 TFEU to create a framework to ensure the free movement of information society services between the Member States. Monitoring injunctions would cause significant expenses on online service providers thus in practice such measures could be impossible to carry out without unjust interfering to online service providers’ freedom to conduct their business as protected by Article 16 of the Charter. Moreover, the general monitoring obligation ban is closely related to the liability exceptions provided for by Articles 12, 13 and 14 of the eCommerce Directive. According to Montero and Van Enis benefit from liability exemptions “would have been reduced virtually to nil if they had not been supplemented by the principle of a ban on any general monitoring obligation”.

However, Article 15 does not prohibit injunctions which do not include general monitoring adopted by national authorities on online service providers. Article 15(2) provides for that the ban set out by Article 15(1) does not preclude obligations set out by national law to provide information to competent authorities at their request or in case alleged illegal activities are undertaken. Recital 45 of the directive provides national authorities possibility to set out injunctions requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it. According to Recital 47 monitoring obligations may be imposed in “specific cases”.

95 See Montero—Van Enis 2011 p. 27.
96 See I bid p. 28—29.
97 Montero—Van Enis 2011 p. 28; see also Lodder—Kaspersen 2002 p. 89.
According to the study Markt/2006/09/E to the Commission injunctions imposed on online service providers have caused unease across the Europe. The study points out several common problems which the Member States have to deal with, such as lack of feasibility of filtering and blocking techniques and the question of proportionality of the issued injunctions.\(^98\) Moreover, monitoring measures has aroused interest within market players\(^99\). This chapter aims to review different types on injunctions and clarify the scope of general monitoring ban of the eCommerce Directive in the light of EU case law and review applicable principles used in assessment.

### 3.1 Injunctions to protect intellectual property rights

The prerequisites for admissible specific monitoring measures in order to prevent intellectual property infringements are completed by the Directive 2004/48 on the enforcement of intellectual property rights (hereinafter Enforcement Directive). According to Article 3 of the Enforcement Directive the measure must be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse. The aims behind the prerequisites are originating from social and economic aims of the internal market as set out in Article 3(3) TEU.

The Member States may set out injunctions on online service providers in order to protect intellectual property rights in certain conditions. According to Article 8(3) of the Directive 2001/29 on the harmonisation of certain aspects of copyright and related rights in the information society the Member States shall ensure that right holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right. Article 3 of the Enforcement Directive limits allowed measures to those which are not unnecessarily complicated or costly, or which do not entail unreasonable time-limits or unwarranted delays. These conditions are confirmed by the ECJ in \textit{Scarlet Extended v. SABAM and others} concerning an injunction to set out a system that would filter all electronic communications transmitted via its services, in particular those involving the use of P2P software, for unlimited time in order to prevent any future infringement of intellectual property rights.\(^100\)

\(^{98}\) See Study on Internet Intermediaries Markt/2006/09/E to the Commission p. 20—22.

\(^{99}\) Edwards has noted the trend according to which powerful industry players tend to favour filtering obligations over notification procedures in combating illegal activities in online environment (Edwards 2009 p. 81).

\(^{100}\) C-70/10 \textit{Scarlet Extended v. SABAM and others} [2011].
Article 11 of the Enforcement Directive imposes obligation on the Member States i) to ensure that judicial authorities may issue an injunction against the infringer of intellectual property rights aimed at prohibiting the continuation of the infringement, and ii) to ensure that the right holders may apply for an injunction against intermediaries. According to Advocate General Jääskinen in his opinion in L’Oréal and others v. eBay the Enforcement Directive does not include any obstacle to set out such injunctions against an intermediary that require the prevention of the continuation and repetition of a specific infringement if such injunctions are available under national law. Jääskinen represented “a double requirement of identity” which includes two requirements for injunctions repetitive cases: i) the infringing third party should be the same and ii) the trade mark infringed should be the same in the cases concerned.101

Since the topic of the thesis refers to making a review of current developments, the EU’s approach towards Anti-Counterfeiting Trade Agreement (ACTA) deserves brief review. The EU has supported ACTA in its intellectual property right policy102 and it was already on its way to accession until the European Parliament voted against it on 4 July 2012. Apparently, the plan went down mainly because the Parliament could not alter the agreement but only approve or block it. Earlier the Parliament had considered referring ACTA to the ECJ in order to assess its incompatibility with the EU fundamental rights law.103 Therefore ACTA is not applied in EU or its Member States.

3.2 How to distinguish specific and general monitoring?

First of all, it have been pointed out by some legal studies that monitoring of content in specific cases cannot be regarded as an exception to the general monitoring ban.104 Montero and Van Enis regard possibility to issue specific monitoring obligation as “supplementing the principle of a ban on general monitoring measures without contradicting it”105. Distinguishing general monitoring ban from monitoring in specific cases is important premise in the analysis since there are significant difference between exclusion and exception. Based on the wording of Article 15 of the eCommerce Directive the prohibition concerns namely general monitoring obligations by setting out a clear rule which effects on possibility of

---

102 Factsheet of the Commission: What ACTA is about?
104 See Opinion of AG Jääskinen in case C-324/09 L’Oréal and others v. eBay paragraph 136; and Montero—Van Enis p. 30. According Van Eecke possibility to issue a specific monitoring obligation constitutes an exception to the general prohibition: see Van Eecke 2011 p. 1486
national authorities to introduce measures in accordance with national law. Specific monitoring is not exception of the ban since the ban does not concern monitoring obligations in a specific case as explicitly stated by recital 47:

“Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation.”

Because of the above-mentioned requirements any injunction on service provider must be justifiable and prescribed by national law but also specified. Moreover as stated by the ECJ, the obligation imposed must be in a fair balance between the various fundamental rights protected by the EU legal order in accordance principle of proportionality. Van Eecke suggests that due to information asymmetry to which the online intermediaries are subject, a national authority must define clear criteria for injunctions. Montero and Van Enis clarify these criteria as follows: “it only seems possible to envisage a form of injunction that involves specific acts of removal, blocking or filtering relating to an infringement, or risk of infringement, which is identified, clearly circumscribed and duly established.”

3.3 How to distinguish illegal content?

The wording of Article 15(1) of the eCommerce Directive refers to seeking facts and circumstances indicating illegal activity. Smith considers this reference unfortunate because it could make an impression to connote only to criminal liability. He reminds that the intent of the directive is to be applicable to civil liability as well. When discussed on illegal content on the Internet in more general context, the discussion often regards to illegal and harmful content. For example, the Communication from the Commission on illegal and harmful content on the Internet given in 1996 refers to both illegal and harmful content. According to Akdeniz the difference between these two is that “the former is criminalized by national laws, while the latter is considered offensive, objectionable, unwanted, or disgusting by some

people but is generally not criminalized by national laws”\textsuperscript{111}. Since the context of the thesis is applying rules originating from the eCommerce Directive, this review concentrates on illegal material which is not restricted only to illegal material in means of criminal law. Illegality of content or activity is usually defined in accordance with national material law.

According to the Commission illegal content could contain for example “infringements of intellectual property rights (such as trademark or copyright infringements), but also sites containing child pornography, racist and xenophobic content, defamation, incitements to terrorism or violence in general, illegal gambling offers, illegal pharmaceutical offers, fake banking services (phishing), data protection infringements, illicit tobacco or alcohol advertisements, unfair commercial practices or breaches of the EU consumer rights acquis”\textsuperscript{112}. When the activity is within the scope of any harmonised provisions of the EU law or the material is illegal \textit{per se}, it should be quite easy to perceive unlawfulness by a diligent service provider\textsuperscript{113}. The Commission has suggested that term “manifestly”, as it have been defined further by national case law, could be helpful in interpretation of the eCommerce Directive\textsuperscript{114}.

A common problem with monitoring measures concerns cross-border nature of the Internet. Lawful and illegal content is not always easy to distinguish in international context. Despite the harmonisation in telecoms and intellectual property rights sector, the Member States have wide margin to impose differing substantive requirements which leads to the situation where certain content is lawful in one Member State and illegal in another Member State\textsuperscript{115}. In order to cope with legal uncertainty, there are two different approaches which should be taken into consideration, \textit{country of origin} and \textit{country of receipt}. The former is an important element of the eCommerce Directive.

\textit{3.3.1 Country of origin principle}

The country of origin principle limited to the internal market has been included to the eCommerce Directive.\textsuperscript{116} According to Trzaskowski this principle consists of two elements: 1) \textit{principle of home country control} and 2) a \textit{principle of mutual recognition}. To be able to apply home country control, apparently, the home country must be figured out at first.

\textsuperscript{111} Akdeniz 2010 p. 262.
\textsuperscript{112} Commission Staff Working Document SEC(2011) 1641 final p. 25.
\textsuperscript{113} See section 2.2.3 of diligent economic operator interpretation.
\textsuperscript{115} See Smith 2007 p. 911.
\textsuperscript{116} Article 3(1) of the eCommerce Directive.
Location could be quite difficult to define when content is available everywhere. However, “while content on the internet may be everywhere it is not nowhere”117. Pursuant to the eCommerce Directive the question of location shall be solved by adopting the place of establishment concept118. Naturally, the next question concerns how the place of establishment is determined. Recital 19 of the eCommerce Directive sets out general basis for the interpretation:

“The place at which a service provider is established should be determined in conformity with the case-law of the Court of Justice according to which the concept of establishment involves the actual pursuit of an economic activity through a fixed establishment for an indefinite period; this requirement is also fulfilled where a company is constituted for a given period; the place of establishment of a company providing services via an Internet website is not the place at which the technology supporting its website is located or the place at which its website is accessible but the place where it pursues its economic activity; in cases where a provider has several places of establishment it is important to determine from which place of establishment the service concerned is provided; in cases where it is difficult to determine from which of several places of establishment a given service is provided, this is the place where the provider has the centre of his activities relating to this particular service.”119

According to recital 19 the significant factor in the assessment is the place where an online service provider pursues its activities. Thus the place of establishment of the service provider who provides services via its website is not necessary the place where servers are located or the place where the website is accessible. The place of establishment is the place where it de facto pursues its economic activity. In accordance with the country of origin principle the supervision of the online providers’ activities should be conducted in the place where the activities are pursued. Therefore a Member State must look after those service providers which conduct their businesses in the area of the concerning Member State. The supervision is based on mutual recognition principle whereas a Member State can rely that other Member States take care of the supervision on their areas as well.120

119 Italics writers.
But where exactly the country of origin principle applies? According to Article 3(1) of the eCommerce Directive the principle applies in “the coordinated field” which is defined Article 2(h) as:

Article 2

h) ‘coordinated field’: requirements laid down in Member States’ legal systems applicable to information society service providers or information society services, regardless of whether they are of a general nature or specifically designed for them.

(i) The coordinated field concerns requirements with which the service provider has to comply in respect of:

- the taking up of the activity of an information society service, such as requirements concerning qualifications, authorisation or notification,
- the pursuit of the activity of an information society service, such as requirements concerning the behaviour of the service provider, requirements regarding the quality or content of the service including those applicable to advertising and contracts, or requirements concerning the liability of the service provider;\(^\text{121}\)

(ii) The coordinated field does not cover requirements such as:

- requirements applicable to goods as such,
- requirements applicable to the delivery of goods,
- requirements applicable to services not provided by electronic means.

In the coordinated field defined above, the country of origin rule is not unexceptional taking into account competence of the EU\(^\text{122}\) and rules of international private law. For example, there are exceptions regarding contractual obligations, copyright, neighboring rights and industrial rights. In addition, the Member States have a right to impose restrictive measures which are proportional and necessary for reasons of public policy, in particular the prevention, investigation, detection, and prosecution of criminal offences, including the protection of minors and the fight against any incitement to hatred on grounds of race, sex, religion or nationality, and violations of human dignity concerning individual; the protection

\(^{121}\) Italics writers.

\(^{122}\) See Article 5 TEU.
of public health; public security, including national security and defence; the safeguarding of the protection of consumers, including investors. Moreover, taking into account Article 1(4), the country of origin rule can be abandoned if contract parties have right to choose the applicable law in accordance with international private law rules. According to Mäntysaari receipt-orientated approach tends to dominate in contractual relations. In consumer contracts applicable law is determined as agreed between parties or when there is no any reference to the applicable law included to the agreement usually the law of consumer’s domicile will be applied.

Hellner considers the relation between the country of origin rule and private law rules uncertain. According to him the country of origin rule cannot be a choice of law rule if Article 1(4) of the eCommerce Directive is taken seriously since the article explicitly says that the directive does not establish additional rules on private international law. Hellner comes into the conclusion that Article 3 of the eCommerce Directive effects similarly as a choice of law rule, even if it is not that “in name and theory”, designating the country of establishment of an online service provider as applicable to some private law issues. In eDate Advertising the ECJ confirmed that Article 3(1) should not be interpreted as a conflict of laws rule and “that paragraph principally imposes on Member States the obligation to ensure that the information society services provided by a service provider established on their territory comply with the national provisions applicable in the Member State in question which fall in the coordinated field”. Therefore instead of imposing a conflict of laws rule Article 3(1) allocates the regulatory authority and imposes a duty of supervision upon the Member State in which the service provider is established.

3.3.2 Harmonisation of criminal law within the EU

Criminal law is traditionally considered as a matter of national law. Within Lisbon Treaty the pillar system was abolished and the content of third pillar including criminal matters was incorporated into to the main body of the Treaty. According to Article 4(2)(j) TFEU area of freedom, security and justice is under shared competence between the EU and the Member states. Shared competence is defined in Article 2(2) TFEU:

---

123 These exclusions relates to competence of the EU in accordance with Article 5 TEU. See Article 3(4) of the eCommerce Directive; and Bergkamp 2003 p. 35.
124 See Mäntysaari 2003 p. 342; and Smith 2007 p. 940.
“When the Treaties confer on the Union a competence shared with the Member States in a specific area, the Union and the Member States may legislate and adopt legally binding acts in that area. The Member States shall exercise their competence to the extent that the Union has not exercised its competence. The Member States shall again exercise their competence to the extent that the Union has decided to cease exercising its competence.”

What comes to substantive criminal law, the EU has competence to adopt binding acts only in the limited area that is defined in Article 83 TFEU. The EU may adopt rules for example concerning serious crime with cross-border dimension like terrorism, trafficking persons, child pornography, drug trafficking etc.\textsuperscript{128}

There are few framework decisions of the Council of the European Union (hereinafter Council) which seek to contribute cooperation in combating illegal online material. The Council has given the \textit{Framework Decision on combating the sexual exploitation of children and child pornography} in 2003 according to which the Member States must take necessary measures to make punishable \textit{inter alia} distribution and possession of child pornography and making it available whether undertaken by means of a computer system or not.\textsuperscript{129} Later in 2011 the Framework Decision was replaced by the Directive 2011/92 which sets out more precise requirements for the minimum rules concerning offences and punishments for sexual abuse and sexual exploitation of children and child pornography. The new directive includes precise definitions of punishable distribution and possession and making available child pornography in Article 5.

Furthermore, the Framework Decision on combating racism and xenophobia adopted in 2008 is designed to ensure that offences concerning racism and xenophobia are punishable in all the Member States by effective, proportionate and dissuasive criminal penalties\textsuperscript{130}. The EU has enacted Action Plan on combating terrorism as revised in 2006 to deepen the international

\textsuperscript{128} See Craig—De Búrca 2011 p. 931—933, 947and 954—956.
\textsuperscript{129} Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography Article 3(1).
\textsuperscript{130} Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law Articles 1(1) and 3(1).
consensus and enhance international efforts to combat terrorism. However, the discussion on role of online service provider in anti-terrorism work of the EU seems to be unfinished.

In the area which lacks harmonisation some of the basic principles provide the starting point. The country of origin principle applies to public requirements as well and therefore the law of the place of establishment applies regardless of where the activity is directed. As referred above, based on Article 82 TFEU mutual recognition applies to criminal matters as well. For example in case of claims regarding defamatory content the question whether the content is defamatory should be solved, when necessary, in a competent national court. Defamation is classically criminalised in national criminal laws but it can be matter of civil law as well. For the online service provider assessment could be challenging since the service provider should at first solve the question of competence and then the substantial law. The eCommerce Directive does not provide much of guidance since it does not aim to harmonise the field of criminal law. Moreover, the eCommerce Directive does not offer any shield for taking down material which the service provider considers illegal but which appears to be lawful. However, the directive does not include obstacles to impose injunctions to take down defamatory content by national court or other national authority.

3.4 Proportionality of injunction

As referred in the ECJ case law regarding intellectual property rights breaches and liability of online service providers, the measures imposed in order to protect rights of others must be in a fair balance between various rights in accordance with the principle of proportionality which is one of the general principles of community law.

Principle of proportionality was developed by the ECJ case law and is currently considered to be applicable in EU law in its entirety. The three most essential elements of the principle are

---

131 See the EU action plan as revised.
133 See Trzaskowski 2005 p. 95.
134 See Van Eecke 2011 p. 1467. It should be noted that defamation is not criminalized in all legal orders. For example UK has decriminalized defamation on 12 November 2009 by Article 73 of Coroners and Justice Act 2009.
135 Recitals 8 and 47 of the eCommerce Directive.
137 C-275/06 Promusicae v. Telefónica [2008] paragraph 70.
1) applicability to intended legitimate aim, 2) necessity of the measure and 3) fair balance between various interests.\textsuperscript{138}

The above-mentioned division is close to Alexy’s model. According to Alexy the principle of proportionality consists of three sub-principles: the principles of suitability, of necessity, and of proportionality in its narrow sense. He considers these principles as expressions of the idea of optimisation, two former relative to the extent what is factually possible and the last relative to legal possibility.\textsuperscript{139}

According to recital 41 the eCommerce Directive the directive strikes a balance between different interests.\textsuperscript{140} The ECJ has assessed proportionality of the injunction issued on a service provider in its case law by balancing different interests at stake.

In \textit{Scarlet Extended v. SABAM} the ECJ considered contested filtering injunction at stake not only resulting in a serious infringement of the freedom of the service provider to conduct its business but also infringement of the fundamental rights of service provider’s customers, namely right to protection of their personal data and their freedom to receive or impart information.\textsuperscript{141} The measure, introducing general filtering system, was considered not being proportionate to the intended objective. The ECJ stated an injunction to introduce the contesting filtering system precluded in the light of applicable directives and fundamental rights.\textsuperscript{142}

The aim is to reach a situation in which different fundamental rights are optimised i.e. respected simultaneously as far as possible. In other words this means that the aim is to secure as well as possible rights of each person.\textsuperscript{143} Principle of proportionality is the tool provided for by EU law which is essential in balancing interests at stake. The interests i.e. protected rights regarding to injunctions issued on online service providers are namely right to property (including intellectual property rights), freedom to conduct a business, freedom of expression and protection of personal data. According to Article 6 TEU there are three primary sources of EU human rights law — the Charter, the ECHR and general principles of EU law. The

\begin{itemize}
  \item \textsuperscript{138} See Laakso 1999 p. 1082—1083.
  \item \textsuperscript{139} Alexy 2005 p. 572—573.
  \item \textsuperscript{140} Recital 41 of the eCommerce Directive.
  \item \textsuperscript{141} C-70/10 \textit{Scarlet Extended v. SABAM} [2011] paragraph 50. Protection of personal data, freedom of expression and freedom to conduct a business are protected by Charter of Fundamental Rights of the European Union which has the same legal value than the Treaties of the EU (Article 6(1) TEU).
  \item \textsuperscript{142} See C-70/10 \textit{Scarlet Extended v. SABAM} [2011] paragraph 54.
  \item \textsuperscript{143} See For example Innanen—Saarimäki 2009 p. 27.
\end{itemize}
Charter has nowadays the same legal value than the Treaties of the EU\textsuperscript{144}. The Charter provides protection equivalent to the ECHR but does not prevent EU law from providing more extensive protection\textsuperscript{145}. The ECHR has been treated as a “\textit{special source of inspiration}”\textsuperscript{146}.

In European electronic communications field, the \textit{openness of the Internet principle} should be taken into account as well.\textsuperscript{147} It is not a right of any individual but it is one reflection of freedom to receive and impart information. According to the Commission Declaration, given in 2009, in relation to revision of common telecoms framework, net neutrality is considered as policy objective and regulatory principle of the common telecom framework.\textsuperscript{148} Article 8(4)(g) of the Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services as amended by Directive 2009/140/EC (hereinafter Framework Directive) includes a general aim to promote “the ability of end-users to access and distribute information or run applications and services of their choice”. Articles 20(1)(b), 21(3)(c) and 21(3)(d) of the Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services as amended by directive 2009/136/EC (hereinafter Universal Service Directive) complete openness principle by setting out transparency requirements in relation to the information that must be provided to end users of electronic communication services.

\textit{3.4.1 Balancing fundamental rights}

At this point, balancing of fundamental rights deserves some further attention. According to the Kiikeri’s “\textit{rule principle}” a right includes an obligation to respect rights of others. Therefore in accordance with the principle of proportionality the right included to the rule must be in proportion with other rule through obligation to respect rights of others.\textsuperscript{149} In context of an injunction issued on the online service provider this would mean that the right of copyright owner (right to property) includes obligation to respect the right of service provider (right to conduct a business) in proportionate way while the rights of third parties (freedom to

\textsuperscript{144} Article 6(1) TEU.
\textsuperscript{145} Article 52(3) of the Charter.
\textsuperscript{147} See Innanen—Saarimäki 2009 p. 35—36.
\textsuperscript{148} See Commission Declaration on Net Neutrality 2009/C 308/02.
\textsuperscript{149} Kiikeri 2012 p. 546.
receive and impart information and protection of personal data) must be protected simultaneously.

In US freedom of speech has been considered prevailing over other users’ interests except when intellectual property interests are at stake.\textsuperscript{150} In European human rights law freedom of expression is considered as one of the essential foundations of a democratic society and one of the basic conditions for its progress\textsuperscript{151}. In the context of this thesis, freedom of expression can be considered having an essential role in interpretation of the dual ban provisions as one of the aims the concerning provisions contribute. However, it cannot be considered having such a weight that would go beyond intellectual property rights or protection of personal data. However, intellectual property right or protection of personal data cannot either be considered as a primary right. In \textit{Scarlet Extended v. SABAM} the ECJ considered that there is nothing in the wording of Article 17(2) of the Charter or in the ECJ’s case law to suggest that that right is inviolable and must be absolutely protected.\textsuperscript{152} In \textit{Promusicae} the ECJ considered that “directives 2000/31, 2001/29, 2004/48 and 2002/58 do not require the Member States to lay down [...] an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings”\textsuperscript{153}. Balancing between freedom of expression and copyrights has aroused discussion in Europe along with cases concerning The Pirate Bay online service. After being convicted for copyright violations in Sweden the administrators of the service took their case before the ECtHR. In given decision \textit{Neij and Sunde Kolmisoppi v. Sweden}, the ECtHR considered balancing of interests (namely freedom to receive and impart information and necessity to protect copyrights) by national courts rightful in the concerning convictions for copyright violations\textsuperscript{154}.

Instead of building any model for hierarchy of fundamental rights, it should be born in mind that national courts should concentrate on balancing the interests at stake carefully in each case based on all the characteristics of concerning case and justify decisions adequately.\textsuperscript{155} Interpretation that gives prevalence for one right over others would be likely to lead to unreasonable results since each case has its own characteristics. The importance of duly

\textsuperscript{150} See Stalla-Bourdillon 2010 p. 494—496.
\textsuperscript{151} Castells v. Spain no. 11798/85 [1992] paragraph 42.
\textsuperscript{153} C-275/06 Promusicae v. Telefónica [2008] paragraph 70.
\textsuperscript{154} Neij and Sunde Kolmisoppi v. Sweden no. 40397/12 [2013].
\textsuperscript{155} This is taken into account in recital 17 of the Enforcement Directive: “The measures, procedures and remedies provided for in this Directive should be determined in each case in such a manner as to take due account of the specific characteristics of that case, including the specific features of each intellectual property right and, where appropriate, the intentional or unintentional character of the infringement.”
justification has become apparent by the ECtHR cases concerning recent Finnish freedom of expression rulings where the ECtHR has condemned Finnish courts of insufficient grounding regarding restricting freedom of expression in order to protect privacy of individuals. In optimising process all the elements of proportionality should be taken into account: legitimate aim, necessity and fair balance between interests. Moreover, this should become clear from grounding of decisions.

3.4.2 Restrictions of fundamental rights

As referred before, a right includes a duty to respect rights of others. This is the essence of balancing between different interests. Balancing requires restricting fundamental rights since different rights cannot be fully ensured simultaneously. Restrictions on fundamental rights in European context must meet certain requirements set out by the Charter and the ECHR.

Article 52(1) of the Charter contains so-called general derogation clause which indicates acceptable restrictions on fundamental rights provided by the Charter. At first, any restriction on charter rights and freedoms must be “provided for by law and respect the essence of those rights and freedoms”. Secondly, limitation must comply with principle of proportionality and be made only if necessary and “genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others”. Article 10(2) of the ECHR includes a specific restriction clause regarding restrictions on freedom of expression:

“The exercise of these freedoms, since it carries with it duties 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.”

The “rule principle” is included to Article 10(2) by bounding exercise of freedoms, including to the freedom of expression, with duties and responsibilities it carries. According to Kiikeri

---

156 Jokitaipale and others v. Finland no. 43349/05. In Jokitaipale and others (paragraph 80) ECtHR stated following: “In conclusion, in the Court’s opinion, the reasons relied on by the domestic courts, although relevant, were not sufficient to show that the interference complained of was “necessary in a democratic society.”

the third party who must solve the conflict is in western democratic societies, in accordance with principle of democracy, an institutional lawmaker who protects and forms rules in order to solve legal relations. Admissibility of restrictions is finally determined by such an institutional actor who solves relation between implicit and other obligation included to a rule and/or other right explicitly formed by the lawmaker. In EU law the ECJ has competence to give preliminary rulings which are, pursuant to the principle of supremacy, binding instructions for interpretation of EU law. Therefore the ECJ plays the role of an actor who solves the relation between interests by having two effects. As a preliminary ruling it solves a question of rightful interpretation of EU legislation in concerning single case but also sets out model for interpretation of EU law to all the Member States. The ECtHR has a different role. According to the Article 46(1) of the ECHR the parties of the convention must undertake to abide by the final judgment of the ECtHR in any case to which they are parties. There are no any direct effects on other contracting parties than those involved to the judgment but the judgments have certain indirect effects. Meaning of the ECHR for individuals in need of protection is the way national authorities apply human rights provisions of the convention.

In conclusion, in conformity with EU law as supervised by the ECJ, the principle that solves whether the injunction at stake is justified and different rights in a fair balance is the principle of proportionality. This principle includes that injunctions imposed on online service providers should be in a fair balance to the legitimate aim while not causing an unjust restriction on any rights at stake or violate openness of the Internet. There is no any special order between the referred fundamental rights thou the balancing must be carried out in each individual case. In the following sections of this chapter is reviewed proportionality of the typical measures imposed on service providers.

3.5 Techniques and procedures

3.5.1 Filtering systems

Filtering systems are defined as software programs which stop certain types of Internet content or certain sites from being accessed by a user. Filtering systems can be applied by

---

159 See Article 267 TFEU of preliminary rulings and section 1.2 of the principle of supremacy.
160 Husa 2001 p. 47.
users for themselves or for other users, for example children, or it can be applied by a service provider for all the users of a service.\textsuperscript{161}

Reasons why the Member States and market players are willing to compel intermediaries to take filtering and monitoring measures are diverse. These days in addition to online piracy for example terrorism, disseminating child pornography and threats to the Internet security, as viruses and malware, have caused changes in approaches towards interfering intermediaries’ activities. According to Edwards presumption that an intermediary is not liable activities of third person is disregarded.\textsuperscript{162}

Despite of the changed approaches, general filtering obligations are clearly precluded in EU law. As referred before, according to the ECJ injunctions to impose general filtering systems in order to prevent breaches of intellectual property rights have been considered not proportionate and therefore precluded in light of EU law.\textsuperscript{163} The Committee of Ministers of the Council of Europe has given recommendation CM/Rec(2012)3 on the protection of human rights in regard with search engines according to which search engine providers should not be obliged to monitor their networks and services proactively in order to detect possibly illegal content, nor should they conduct any \textit{ex ante} filtering or blocking activity, unless mandated by a court order or by a competent authority.

According to several studies limited filtering systems should not be either accepted without further consideration. A limited filtering measure would not be likely to lead to the aimed result, division between lawful and illegal content, because of practical reasons. Up-keeping a filtering measure requires plenty of resources and moreover blocks (which could be included to the filtering system) are possible to evade by using technical measures, like encryption and bypassing schemes.\textsuperscript{164} Furthermore, a filtering measure may easily breach protected fundamental rights if it is not in fair proportion to its aim. The ECJ has pointed out that filtering systems of online service providers would involve the identification and processing of protected personal data connected with the profiles created on the social network by its users.\textsuperscript{165} Moreover, one may say that since filtering measures may not be feasible in light of

\begin{itemize}
\item Edwards 2000 p. 297.
\item See Edwards 2009 p. 83—84.
\item See Study of Internet blocking balancing cybercrime responses in democratic societies p. 199; and Abbott 2009 p. 6.
\end{itemize}
applicable techniques such measures should be approached with carefulness. The situation may become different within further development of available techniques. So-called deep packet inspection tools have already raised enthusiasm towards their exploitability.\footnote{166}{Edwards has referred to the “increasing sophistication of deep packet inspection” (Edward 2009 p. 83).}

3.5.2 Blocking

Blocking measures, as means of removing or disabling access to certain content, have been in practice directed to individual files but also to entire web sites or even to groups of sites. Blocking may be applied by own initiative of a service provider or as result of an order of a court or other authority.

One extreme example is ECtHR case Ahmet Yildirim v. Turkey in which the national court had accepted blocking of Google Sites as whole in order to block access to one particular site that included defamatory considered material. The measure was justified by national court as considered being only way to block the site in question. According to ECtHR such a measure was restriction on Internet access and therefore it restricted freedom of expression provided by Article 10 of the European Convention on Human Rights.\footnote{167}{Ahmed Yildirim v. Turkey no. 3111/10 [2012].} In this case lack of fair balance between the interests was clear. Usually lack of balance is not that clear.

Blocking measures which are directed to entire web sites have been opposed by the EU and the Council of Europe. The main arguments against general blocking measures are that such measures would not guarantee human right standards and that they would not be adequate since the web site may re-appear in another location outside of EU jurisdiction.\footnote{168}{See Commission Staff Working Document SEC(2007) 1424 of 6 November 2007. The Council of Europe has expressed its opposition towards general blocking or filtering measures in Recommendation CM/Rec(2008)6.} Blocking restricts freedom of expression protected by Article 11(1) of the Charter according to which everybody has freedom to impart and receive information and ideas without interference by public authority and regardless of frontiers. As it has become apparent, this right is not absolute. Recently, there has been imposed restriction of the said freedom in the EU level regarding limited field under the competence of the EU. Article 83 TFEU provides the European Parliament and the Council possibility to establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension, as sexual exploitation of women and children. In the end of 2011 the Council adopted the Directive 2011/92 on combating sexual abuse and exploitation of children and child pornography which allows Member States to take measures to block...
access to web sites which contain or disseminate child pornography towards the Internet users within their territory. Imposing such a blocking measure presumes transparent procedures and adequate safeguards to ensure that the restriction is necessary and proportionate including possibility for judicial redress. Further the users must be informed of the reason for the restriction.\textsuperscript{169}

In general, blocking of websites has aroused opposition among legal studies. According to Abbott removal of illegal content by hosting service will always be more efficient than nationwide attempt\textsuperscript{170}. Akdeniz comes into conclusion that state level blocking measures are inadequate in combating illegal content. According to him “\textit{circumvention technologies are developed hand to hand with blocking and filtering technologies and Internet users are capable of circumventing blocking mechanisms and accessing supposedly blocked pages as long as those pages continue to be available over the Internet and not taken-down by those who host them}”\textsuperscript{171}. Van den Bogaert and Cuyvers have a little more optimistic approach towards feasibility of blocking measures. In context of online gambling (which is excluded from the scope of eCommerce Directive) they encourage EU to contribute cooperation – “\textit{by forming one block, the EU can thereby form a much more effective force in dealing with the realities of online services, and can enlist, rather than challenge, the technological know-how and resources of legitimate suppliers}”\textsuperscript{172}.

Blocking of individual files is not usually problematic in case the unlawfulness of the content is apparent, especially if a court has balanced interests carefully before imposing an injunction. However, it should be taken into account that any measure imposed should be feasible. Article 3 of the Enforcement Directive requires that the measures imposed by the Member States in order to protect intellectual property rights are effective, proportionate and dissuasive. A measure that is not effective cannot be proportional either. The problem of blocking techniques is that despite of the measure the content stays on the Internet and therefore it is accessible in the way or another for those who have interest to get access to it.


\textsuperscript{170} Abbott 2009 p. 6.

\textsuperscript{171} Akdeniz 2010 p. 269.

\textsuperscript{172} Van den Bogaert and Cuyvers consider feasibility of Domain Name System (DNS) filtering and Internet Protocol (IP) filtering in their article about ECJ case law regarding gambling. Van den Bogaert—Cuyvers 2011 p. 1211—1213. However, gambling including games of chance, lotteries and betting transactions, which involve wagering a stake with monetary value are excluded from the scope of the eCommerce Directive (recital 16 of the directive).
In other words, available blocking techniques, instead of enabling the access, in reality they actually just make accessing to the content a little more difficult.

3.5.3 Other traffic management measures

There are several other measures pursued in the telecom markets, like throttling, prioritisation, etc. which may be directed on specific types of traffic (protocols) or content. Instead of being utilised as injunctions imposed by national authorities, these traffic management measures are more likely to be imposed on own initiative of service or network providers. Typically these measures are used by network operators for ensuring smooth flow of traffic by avoiding networks from getting congested, which is necessary for the proper functioning of networks. On the other hand, these measures may be used in problematic way for limiting certain band-consuming services like voice over Internet protocol (VoIP) or P2P services. The potential abuse of traffic management has aroused concern among the Member States and the market players.\(^{173}\) Traffic management measures are not prohibited in the light of EU law but they must comply with the provisions provided for by national and EU law.

3.5.4 Lack of feasibility of injunctions

Injunctions issued by the Member States should be adequate in order to fulfill the requirement of proportionality. An ineffective injunction is likely to restrict a service provider’s right to conduct business provided for by Article 16 of the Charter and the user’s right to receive and impart information provided for by Article 11 of the Charter. An ineffective injunction, that does not fulfill the legitimate aim, cannot fulfill requirement of necessity and fair balance between rights. Therefore, an injunction should be feasible in order to be proportionate.

What comes to technical matters as it has become clear within the thesis, there are several questions to be solved regarding to filtering and blocking obligations issued on service providers. At first, it must be figured out how to introduce an injunction without unreasonable expenses and delay. In general, available techniques for general monitoring are not considered feasible based on the state of art of technology. This became apparent in SABAM v. Netlog in which the ECJ stated that filtering system in question “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”.

Secondly, sharers of illegal content have ways to bypass blocks by using various techniques. When used techniques are found and blocked, skillful users of the Internet start to invent new techniques and service providers tend to transfer their activities into another address. Judgment and decisions concerning certain sites and they generally cannot have effect on a new domain by which a service provider makes blocked content available again. The question is, are the filtering or blocking measures able to lead to the intended result after all this? As mentioned before, among legal studies the approach towards effectiveness of filtering measures has been quite reserved even regarding to specific filtering measures. Since there is no consensus of applicable techniques, proportionality and feasibility must be assessed before imposing the injunction in order to evaluate whether an injunction in question fulfill requirements of the principle of proportionality.

Among legal studies it has been suggested that developing standards of the applicable measures would improve legal uncertainty in the electronic communication field. These standards could be developed by national courts or, if the case law of courts is not sufficient to form common standards, by standardising committees. Standards could improve legal certainty presuming that various interests have been taken into account when the standards have been determined and that the national courts accept and apply those standards in their case law. Moreover, the standards should be dynamic and reflect the state of art of the available technology. Even though the aim of standardising would be determining fair practices, it seems likely that online service providers would not be willing to contribute attempts to set out barriers between themselves and their customers. On the other hand, it has been argued that hosting providers would benefit from common standards, as they de facto bear the most of the legal risk when being in central position between right holders and users. Moreover, such standards could be functional solution only as far as such standards

175 See Abbott 2009 p. 6; and Montero—Van Enis 2011 p. 34.
176 Montero and Van Enis argue in their study that “imposition of filtering, even if limited, is very likely to be a measure disproportionate to the objective of protecting the rights of holders of intellectual property rights” (Montero—Van Enis 2011 p. 34). Abbott claims that “removal by the hosting service will always be more efficient than nationwide filtering attempt” (Abbott 2009 p. 6).
178 Abbott reminds that file-hosting services are legitimate businesses and “they will not take kindly to anyone putting up blocks between them and their paying customers” (Abbott 2009 p. 6).
are flexible and completed by new innovative techniques that contributes rights of different actors. Do we have such technique available yet on which the standards could be developed?

However, in European level there are no any such standards developed. Thus injunctions should be determined case by case taking into account the specific characteristics of concerning case. Proportionality must therefore be controllable through effective remedies as protected by the Charter.\textsuperscript{180}

3.6 Requirements of net neutrality policy

The European Commission considers success of the Internet stemming from its open and accessible character.\textsuperscript{181} Article 8(4)(g) of the revised Framework Directive includes a general aim to ensure freedom of expression by promoting “the ability of end-users to access and distribute information or run applications and services of their choice”. According to the Commission Declaration, given in 2009 in relation to revision of common telecoms framework, net neutrality is considered as policy objective and regulatory principle of the common telecom framework.\textsuperscript{182} Currently, the European net neutrality debate concerns mainly traffic management measures that are conducted by service providers by way which does not respect rights of users referred above. For example, an access service provider may be willing to avoid disputes by making using of certain services based on user generated content difficult or even throttle using of such services. What comes to measures that may restrict freedom of speech, following two requirements deserve brief review at this point.

At first, online service providers must fulfill transparency requirements set out in the Universal Service Directive. Pursuant to the Article 20(1)(b) information service providers must specify in their end user contracts \textit{inter alia} i) information on any conditions limiting access to and or use of services and applications, ii) any procedures put in place by the information service provider to measure and shape traffic so as to avoid filling or overfilling a network link, and information on how these procedures could impact upon service quality. Article 21(3)(c) and 21(3)(d) of Universal Service Directive provide for national regulatory authorities possibility to impose obligations on service and network providers to inform subscribers of any changes to conditions limiting access to / and use of services and applications and to provide information on any procedures put in place to measure and shape

\textsuperscript{180} Article 47 of the Charter. Equivalent right is protected by Article 13 of the ECHR.


\textsuperscript{182} Commission Declaration on Net Neutrality 2009/C 308/02.
traffic and possible impact upon service quality on those procedures. Pursuant to recital 28 of the Universal Service Directive “end-users should be able to decide what content they want to send and receive, and which services, applications, hard-ware and software they want to use for such purposes”. In BEREC’s guidelines on Transparency in the scope of Net Neutrality the primacy of end user’s perspective is considered as one of the major requirements for a net neutrality transparency policy. To put it briefly, measures in order to shape traffic in online network are not prohibited in general but the use of these measures must be transparent and promote “informed choices” of end users.

Another cornerstone of EU’s transparency policy is effective competition. The aim is to “reduce ex ante sector-specific rules progressively as competition in the market develops”. In other words, competition system exercised in common telecom framework enables imposing ex ante regulatory obligations in those markets which are not considered effectively competitive based on review of national regulatory authorities. Obligations imposed on such markets should be directed only on undertakings with significant market power. The connection between net neutrality and competition in the market has been acknowledged. According to the Commission “the significance of the types of problems arising in the net-neutrality debate is therefore correlated to the degree of competition existing in the market”. Laguna de Paz claims that the main types of measures violating net neutrality do not raise concerns as far as there is efficient competition at network level. Effective competition is taken into account, for example, in Article 3(2) of the Enforcement Directive regarding to enforcement of intellectual property rights by setting out a requirement for measures and procedures to be applied in such a manner as to avoid the creation of barriers to legitimate trade. According to recital 12 the measures provided for in the directive should not be used to restrict competition unduly in a manner contrary to the competition law of the EU.

Even though the core of net neutrality debate regards to activities of network service providers to manage information traffic, the mentioned principles of net neutrality including openness of the Internet requirement should be taken into account in consideration of

---

186 I bid, paragraphs 4—7; and articles 14—16 of the Directive 2002/21/EC as amended on a common regulatory framework for electronic communications networks and services (Framework Directive). ‘Significant market power’ is assessed by national regulatory authorities within their territory.
injunctions on intermediaries as well. It is in user’s interest to know why injunction is imposed and how it effects on using a service. Moreover, injunctions imposed by national authorities on intermediaries should not restrict legitimate trade or effective competition unduly, which should be taken into account when assessing proportionality of the injunction.

4 Notification procedures

The eCommerce Directive leaves online service providers into a contradicting situation — service providers are obliged to expeditiously remove or disable access to illegal material, which the provider is aware of, in order to enjoy liability shield while service providers do not have any applicable shield against claims of their users regarding taking down lawful material in case they did not succeed in assessing illegality.189

The eCommerce Directive provides a possibility to the Member States to impose procedures to remove or disable access to illegal information stored by hosting service provider. Such procedures are commonly called in legal literature as “notice and take down procedures” (hereinafter NTD procedures). So far these procedures are not harmonised in the common market but Article 14(1)(b) of the eCommerce Directive constitutes basis for the development of such procedures.190 The question concerning need for harmonised procedure was left open to wait for re-examination of the directive in accordance with its Article 21. In 2012 the Commission gave an initiative for common procedures for notifying and acting on illegal content hosted by online intermediaries.191

4.1 NTD procedures within Member States

NTD procedures imposed among the Member States vary from formal procedures to self- and co-regulatory procedures.192 This section makes a non-exhaustive review on practices and doctrines which have been introduced in some Members States and evaluations of those.

Some Member States have introduced varying formal, codified NTD procedures.193

189 See Van Eecke 2011 p. 1467—1468.
190 Report COM/2003/0702 from the Commission to the European Parliament, the Council and the European Economic and Social Committee p. 14. According to Article 14(3) of the eCommerce Directive the article does not “affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information”. According to Edwards and Waelden in their WIPO workshop keynote paper Online Intermediaries and Liability for Copyright Infringement p. 28 “Article 14, furthermore, seems to imply that once notice has been given and the expedient period of grace expired, liability is strict even if take-down presents technical or administrative problems.”
191 See section 4.2.
For example, in Finland there is a formal notification procedure prescribed by law which is applicable in copyright and neighbouring right infringements. The Finnish government has also issued a bill which would enable notifying single users of repetitive copyright infringements through a “soft” notification procedure, but the bill has expired so far without any further actions\(^\text{194}\).

There are several advantages of formal procedure. It enhances legal certainty by setting out rules which service providers must follow in order to enjoy liability restriction after being notified of alleged infringing material. For example, such rules may include clarification of what “expeditious removal or disabling access” means in context of Article 14 of the eCommerce Directive. In other hand, it clarifies the question of hosting provider’s awareness which is relevant in evaluation of hosting provider’s liability. Moreover, formal procedure may eliminate the problems concerning assessing of illegality of the content if the procedure includes clear rules of based on which matters the decision to take down material should be made of. Moreover, a notification procedure may clarify such situations when the evaluation of illegality should be brought before a court.

There are two main issues concerning formal procedures. Mere reliance upon official notification by authorities would lead de facto exemption from liability even though there would exist clear awareness of illegal activities\(^\text{195}\). In the context of implementation of NTD procedure in Finland, the Commission has pointed out that in order to enjoy liability restriction a hosting service provider must remove or enable access to illegal information also after attaining information otherwise than by the formal NTD procedure\(^\text{196}\). Another problem concerns formality itself — slow and heavy procedure may not satisfy a right holder or a victim who has an interest to get infringing material taken down as fast as possible.

Instead of formal procedure, the Member States or market players have adopted voluntary notification procedures. Recital 40 of the eCommerce Directive aims to contribute such procedures by stating that the directive “should constitute the appropriate basis for the development of rapid and reliable procedures removing and disabling access to illegal information; such mechanisms could be developed on the basis of voluntary agreements

\(^{193}\) For example Finland, Lithuania, The United Kingdom, Sweden, Spain and Hungary. Study on Internet Intermediaries Markt/2006/09/E to the Commission p. 106—110.

\(^{194}\) HE 235/2010 vp.

\(^{195}\) See Study on Internet Intermediaries Markt/2006/09/E to the Commission p. 15—16.

\(^{196}\) HE 194/2001 vp.
between all parties concerned and should be encouraged by Member States”197. Self-
regulatory codes of conduct are promoted by Article 16(1)(b) of the eCommerce Directive
which states that “Member States and the Commission shall encourage the voluntary
transmission of draft codes of conduct at national or Community level to the Commission”.
Already in 1996 the Commission has considered “encouraging self-regulation between
associations of Internet access providers” as one of the measures which should be taken to
reduce the flow of illegal and harmful content on the Internet198.

Voluntary procedures including self- and co-regulatory measures are common within the
Member States199.

For example, the Austrian Internet Service Providers Association (ISPA) has
developed code of conduct, which is binding for the members of the association,
to specify the applicable NTD procedure. Associations of telecom and other
related industries have developed codes of conduct also at least in Denmark,
France and the United Kingdom. One example of practice applied in several
Member States is eBay’s VeRO program which enables intellectual property
owners to easily report infringements of their intellectual property rights.200

However, if assumption of knowledge would follow a simple notification given by any third
party the risk of abuse of the procedure would rise very high.201 According to the ECJ’s
approach in L’Oréal and others v. eBay, the decision to remove or block content a notification
should be based on sufficiently precise or adequately substantiated information, but the court
must take into account in its evaluation all notices of illegal content or activity which the
provider has received.202 As a comparison to US203, in the Digital Millenium Copyright Act
(hereinafter DMCA) the required elements of notification are defined precisely in the act.
When an intermediary service provider “takes down” the alleged infringing material based on
given notification in good faith it benefits from a so-called “safe harbor” which protects it

197 See also Article 16 of the eCommerce Directive that encourages drawing up codes of conduct.
200 I bid p. 112—113.
201 I bid p. 15—16.
202 See C-324/09 L’Oréal and others v. eBay [2010] paragraph 122: “given that notifications of allegedly illegal
activities or information may turn out to be insufficiently precise or inadequately substantiated, the fact remains
that such notification represents, as a general rule, a factor of which the national court must take account when
determining, in the light of the information so transmitted to the operator, whether the latter was actually aware
of facts or circumstances on the basis of which a diligent economic operator should have identified the
illegality”. See also Van Eecke 2011 p. 1485.
203 It should be noted that the DMCA applies only copyright infringements while possibility to enact notification
procedure based on the eCommerce Directive is not restricted to intellectual property law cases.
from any liability arising from that takedown. In other words, when a service provider has ascertained taking down being formally correct it can be protected by good faith safe harbor.204 In *Lenz v. Universal Music Corp.*, notification procedure was completed by a fair use doctrine according to which a copyright owner must consider fair use before proceeding with a takedown notice under the DMCA205.

Secondly, the voluntary procedures do not solve the issue of legal uncertainty since the illegality is not examined by a court or other authorities before taking down the material. Usually taking down of online material stored involves a risk that the material taken down turn up to be lawful. As referred before, the assessment of unlawfulness may be difficult task for intermediary service provider. Moreover, the eCommerce Directive does not provide any protection for a service provider or a content provider in taking down of alleged illegal material which appears to be lawful.206 The DMCA in turn, provides that a takedown notice must be notified to the “owner” of the material which is to be taken down. Then the owner has an opportunity to intervene the taking down and protest it by a “counter-notice”. If that person disputes that there is copyright infringement then the material in question is “put-back” by the intermediary service provider.207 Counter-notice and put-back option are included to the formal notification procedure for example in Finland as well208.

Most of the issues concerning formal and voluntary NTD procedures may be coped with applicable remedies. In case of intellectual property infringements measures like counter-notice and put-back option have been considered useful in practice. These measures would require rapid preliminary preview proceedings though in order to avoid an abuse of them.209 Despite applicable remedies, if a notification procedure leads to an automatic take down of material alleged illegal the risk of unjust restricting freedom of expression by abusing the notification procedure is high.

It should be born on mind that the eCommerce Directive sets out requirements for service providers to take active measures in order to remove or enable access to illegal content after

204 Section 512(c)1(C) and 512(c)3 of the DMCA. See also WIPO workshop keynote paper Online Intermediaries and Liability for Copyright Infringement p. 29—31.
206 Van Eecke 2011 p. 1467—1468; and WIPO workshop keynote paper Online Intermediaries and Liability for Copyright Infringement p. 32.
207 Section 512(g)(3) of the DMCA; and WIPO workshop keynote paper Online Intermediaries and Liability for Copyright Infringement p. 32.
209 Study on Internet Intermediaries Markt/2006/09/E p. 16.
obtaining awareness of it as a condition for enjoying the liability limitation of intermediaries set out in section 4 regardless formal or voluntary procedures available. However, a notification procedure clarifies the situation of a service provider who seeks to benefit from liability restriction as well as situation of a right holder who wants to enforce his/her intellectual property rights. A notification procedure may also provide remedies for those who happened to be victims of defamatory or other harmful content. At this background, a functional notification procedure seems to be decent option in ensuring legal certainty.

4.2 Harmonised procedure in the EU?

Lack of harmonised procedure has been considered as causing legal uncertainty for the online intermediaries and practical difficulties for the right holders in European level. Based on remarks made in this thesis, such a procedure would significantly strengthen legal certainty and make utilising of the special liability regime easier by clarifying the questions referred above not just national but regional level as well.

Based on the given critique, the Commission submitted an initiative in the beginning of 2012 for horisontal “notice and action procedures” (hereinafter N&A procedures). The term ‘action’ has been chosen because of being in conformity with Article 14 of the eCommerce Directive consisting of removing or disabling access to illegal content by a hosting service provider. The policy objectives of the initiative are i) contributing development of trust and therefore growth in (cross-border) online services; ii) contributing combating illegality on the Internet; iii) ensuring the transparency, effectiveness, proportionality and fundamental rights compliance of N&A procedures; and iv) ensuring a balanced and workable approach towards N&A procedures, with a focus on fundamental rights and the impact on innovation and growth.

According to the initiative, the harmonised procedure is justified by “the cross-border nature of the internet, the existing fragmentation of N&A procedures, the lack of development of regulatory codes in European level and conflicting jurisprudence within and across the Member States”. The initiative is a result of the fact that the notification procedures have been developed almost merely by national legal orders which has led to fractured practices

---

210 Articles 13 and 14 of the eCommerce Directive.
213 Roadmap concerning the N&A initiative p. 1—2.
and legal uncertainty in the common market. For example, as referred in section 2.2.2.2, the Member States have solved the relation between notification procedure and actual knowledge of service provider by varying ways. The common procedure would clarify this relation and abolish diverging practices, and hence contribute legal certainty. Moreover, harmonised notification procedure has been considered as “one of the essential mechanisms through which the eCommerce Directive achieves a balance between the interests of rightholders, online intermediaries and users”\textsuperscript{214}.

However, it may be challenging to prescribe a procedure that would not unreasonably interfere the business of intermediary service providers, would not require large resources from national authorities and would expeditiously prevent access to illegal content. At the moment of finishing the thesis in hand the outcome of the initiative is still unclear.

### 5 Liability of service providers providing peer-to-peer arrangements

P2P arrangements deserve some further attention as a technical innovation which has aroused set of new legal questions. These arrangements, which are commonly used for file-sharing, have aroused several legal problems regarding especially copyrights violations.

The commonly used modern techniques, like BitTorrent protocol, enable easy and fast sharing of large documents. Sharing files via P2P network may be the easiest way to share large files with large amount of recipients.\textsuperscript{215} While such arrangements contribute imparting and receiving online information, on the other hand, they are commonly used for unauthorised file-sharing. Even though the P2P techniques may be used, and are used, in practice for illegal activities it does not mean that the P2P arrangements or use of them would be illegal by definition.

#### 5.1 Definition of P2P

It has been claimed that P2P arrangements fits ill to the definition of hosting service since in modern P2P the content itself is not stored on a server of the hosting provider but on computers of individual users of the service.\textsuperscript{216} P2P is defined in an encyclopedia as “a network consisting of two or more computers that use the same program or type of program

\textsuperscript{214} Van Eecke 2011 p. 1479.
\textsuperscript{215} “\textit{File-hosting services are the most powerful way to distribute large files. There are countless non-piracy reasons for wanting to do this. File-hosting services are the answer to anyone faced with the question of how to distribute a wedding video to a few hundred email addresses.}” Abbott 2009 p. 5.
\textsuperscript{216} See Abbott 2009 p. 3.
to communicate and share data”. The definition follows: “each computer, or peer, is considered equal in terms of responsibilities, and each acts as a server for the others in the network”. The latter part of the definition refers to the modern P2P arrangements which differ from traditional client/server model. In client/server model shared data is stored in central servers which host the shared data. In modern file-sharing an intermediary service provider organises a meeting point between sharers and downloaders of files by providing to the users an online service including search and tracker functions and a database of peers. In other words, in modern P2P arrangements the storage of actual illegal content is pursued outside of the provided service which makes the assessment of a service provider’s liability complicated. This chapter concentrates only on this modern type of file-sharing.

According to a suggestive division there are two primary ways to carry out P2P — centralised and non-centralised arrangements. A centralized arrangement includes a central server which coordinates the traffic between its users although the transfer of files is carried out directly between the users. A central server helps with searching files by locating data and directing connections between users. Non-centralized P2P arrangement does not include any central server but the users connect each other directly. This means that closing down such activities is possible only by closing down all the connected appliances.

For the sake of clarity, commonly used BitTorrent protocol deserves a brief review. Understanding the technical features of the protocol is essential in reviewing recent cases like The Pirate Bay or Finreactor. So-called Torrent files, that owe their name to the referred protocol, indicate the material that is available on other users’ computers to be located and downloaded to the user’s computer. In BitTorrent files are broke into small pieces, and the whole file is downloaded piece by piece from different sources. A service based on BitTorrent assists users to share, trace and download material directly between single computers while no actually illegal material is hosted by the service. Instead, the service hosts Torrent files which include information of the content that is originating from the user who hosts the data on his/her computer. In other words, the service provider does not get actual knowledge of the

---

217 Kajan 2002 p. 399. This definition is not legal.
221 See Frabboni 2010 p. 144.
content since only information of the content is the information that the “hosting” user has given, for example by naming a file.\textsuperscript{222}

In practice P2P arrangements have many variations and techniques develop constantly. It should be born on mind that because in P2P-type file-sharing the techniques and services vary, each service should be assessed individually. None of used techniques or ways of organising the activities is illegal or forbidden \textit{per se}. This premise is justified based on the common aim to promote technical innovations and taking advantage of the state of art of technology as set out in Article 3(3) TEU. In certain national case law liability of an intermediary has been based on complicity to the principal offence which may be for example violation of an intellectual property right or distributing and making available illegal material, like child pornography. Complicity doctrine is reviewed briefly below in section 5.3.

5.2 Requirements stemming from principle of proportionality

So far there is only a little applicable case law of the ECJ concerning P2P arrangements available. The ECJ has not committed itself to the question how a liability of a service provider providing services connected to P2P arrangements should be assessed in relation to illegal content. Those cases regarding more or less P2P arrangements given by the ECJ concern mainly balancing of interests at stake through principle of proportionality.

In \textit{Scarlet Extended v. SABAM} where the plaintiff required the service provider to install filtering system for electronic communication that use P2P software, the ECJ confirmed monitoring ban provided for by Article 15 of the eCommerce Directive applicable to P2P arrangements. The ECJ did not assess further technical questions of the service which uses P2P software, and Advocate General \textit{Cruz Villalón} claimed further technical assessment being an issue of a national court\textsuperscript{223}. However, the ECJ held filtering injunctions to monitor all the electronic communication, in particular those involving the use of P2P software, precluded in the light of EU law, namely in light of Article 15 of the eCommerce Directive and Article 3(1) of the Enforcement Directive\textsuperscript{224}.

The ECJ did not assess particularly whether the online service in question falls within the coverage of Articles 12—14 of the eCommerce Directive even though according to wording of Article 15 the ban concerns providers of said services. Despite of that, the ECJ considered

\textsuperscript{222} Of BitTorrent protocol see website www.bittorrent.com.
\textsuperscript{223} See Opinion of Advocate General Pedro Cruz Villalón in C-70/10 \textit{Scarlet Extended v. SABAM} paragraph 50.
\textsuperscript{224} \textit{C-70/10 Scarlet Extended v. SABAM} [2011] paragraphs 38—54. See section 5.2.
directives 2000/31, 2001/29, 2004/48, 95/46 and 2002/58 when read together having the effect to preclude an injunction made against an intermediary service provider which requires it to install the contested filtering system. Such an interpretation suggests that applicability of the ban provided for by Article 15 is not strictly limited to services that are covered by the special liability regime. The core of general monitoring ban seems to stem from more general principles regarding balancing different interests by virtue of principle of proportionality. Therefore, compared to special liability regime the coverage of the general monitoring ban seems to be broader. In interpretation concerning special liability regime the ECJ has strictly considered it applicable only on providers of those services that fulfill the requirements provided for by Articles 12—14 of the eCommerce Directive.

Another P2P network case considered by the ECJ, *Promuscae* concerns obligation of an Internet access provider to communicate personal data of users in the civil case concerning unfair competition and intellectual property infringements. The ECJ came up with the conclusion that directives that ensure effective protection of copyright (the directives 2000/31, 2001/29, 2004/48 and 2002/58) should be interpreted not requiring the Member States to lay down an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings. In *Promuscae* the ECJ relied on interpretation familiar from *Lindqvist* that the Member States must not only interpret their national law in a manner consistent with those directives in question but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality.

In European level, in means of broader scope than in the EU, proportionality has been discussed by the ECtHR in *Neij and Sunde Kolmisoppi v. Sweden* concerning Swedish *Pirate Bay* case. *Pirate Bay* cases will be reviewed in following sections.

### 5.3 Service provider – offender, abettor or mere intermediary?

#### 5.3.1 Pirate Bay cases in Sweden and Finland

*Pirate Bay* trial in Sweden in 2009 cut a dash around Europe when Swedish courts had to examine liability of search and tracker site provider for copyright infringements. It was one of

---

225 C-275/06 *Promuscae v. Telefónica* [2008] paragraph 70.
the first cases when a trial concerning internationally popular file-sharing service was considered in European perspective. Even though Pirate Bay case has not been examined in supreme court level in Sweden, nor in Finland, the cases should be taken into account in the context of P2P arrangements in European point of view since these cases have aroused wide public discussion. According to Frabboni Swedish Pirate Bay case exposed the weaknesses of the current generation of P2P file-sharing platforms and the risk faced by intermediaries that interact with those platforms.227

The Swedish district court, which considered Pirate Bay case as the first instance, held administrators of the services abettors of the infringements and therefore sentenced them to imprisonment for one year and ordered defendants to pay severe damages to the production companies. The Svea Court of Appeal amended the judgment by shortening prison sentences but making damages even more severe.228 The administrators were not permitted to leave an appeal to the Swedish Supreme Court.

After the Swedish judgments group of production companies, which pursue activities in Finland, applied for a decision before Finnish district court to order the dominant network and service providers to enable access to The Pirate Bay sites in Finland. The Helsinki District Court accepted the applications and the dominant Internet access providers were ordered to enable access to the sites as interim injunction provided for in section 60c(3) of the Finnish Copyright Act (Tekijänoikeuslaki 404/1961) in order to discontinue making of the allegedly copyright infringing material available to the public. One of the Internet access providers DNA, as other service providers as well, appealed of the imposed injunction to the Helsinki Court of Appeal which decided not to annul the orders.229 The network service providers were denied to leave an appeal to the Finnish Supreme Court.

In Sweden Pirate Bay case was first of its kind where the court needed to decide a criminal case concerning an Internet service which has been mainly used and, as held by the court, intended for unlawful purposes.230 The Svea Court of Appeal held administrators of the file-sharing service abettors of the principal offence against copyrights (“medhjälp till brott mot upphovsrättslagen”). The court considered the administrators being aware of copyright infringements based on warning letters and claims that administrators received via e-mail. Moreover, the administrators were considered being aware of all the prevailing circumstances

---

227 Frabboni 2010 p. 142.
228 Svea hovrätt B 4041-09, 17 April 2009.
229 Helsingin hovioikeus no. 383, S 12/1850, 8 February 2013.
that should exist to constitute a copyright infringement.\textsuperscript{231} The administrators of the service pled to the special liability regime by claiming that no illegal material is stored by the service. The Svea Court of Appeal considered in its judgment that the liability restriction, that has been implemented into Swedish electronic commerce law (\textit{Lag (2002:562) om elektronisk handel och andra informationssamhällets tjänster}), was not applicable in the concerning assessment of criminal liability. This conclusion was based on following remarks. \textit{The Pirate Bay} was considered not falling within scope of services provided for by Articles 12 and 13 of the eCommerce Directive since service enabled downloading and hosting Torrent files. Secondly, applicability of Article 14 was not successfully invoked since the claims did not concern information stored to the service but the functions that have contributed acts of users.\textsuperscript{232}

The District Court of Helsinki has taken into account case law of the ECJ and other Member States in its DNA judgment, namely the referred \textit{Pirate Bay} judgment of the Svea Court of Appeal. The district court based its decision to impose the interim measure \textit{inter alia} on the fact that The Pirate Bay still carries on its activities despite of the prison sentences of the administrators and that it is justified to consider that the administrators cannot be heard because of their place of residence is unclear.\textsuperscript{233} The question whether measures, like the interim measure set out by the Helsinki District Court, falls within the scope of allowed injunctions in accordance with the eCommerce Directive would require further review of applied national law. At the first glance, there seems to be no any obstacle since the eCommerce Directive allows, despite of the special liability regime, injunctions based on an order of a court or administrative authorities, requiring termination or prevention of infringements including removal or disabling access to illegal information.\textsuperscript{234} In accordance with the country of origin principle illegality of the content should be assessed and decided based on national law, in this case national criminal and intellectual property laws, which are not reviewed further in this thesis. After all, admissibility of an injunction must be solved through the principle of proportionality.

The Swedish \textit{Pirate Bay} case has evoked discussion concerning evaluation of relation between linking activities and the special liability regime. Linking activities are common in services that host user-generated content. As Edwards has asked, could the law separate

\textsuperscript{231} Svea hovrätt B 4041-09, 17 April 2009, p. 19, 26—27.
\textsuperscript{232} Svea hovrätt B 4041-09, 17 April 2009, p. 49.
\textsuperscript{233} Helsingin hovioikeus no. 383, S 12/1850, 8 February 2013.
\textsuperscript{234} Recital 45 of the eCommerce Directive.
“good” hyperlinkers from bad ones? And if such division is possible, on what basis should it be made? In the light of current state of law, the evaluation should be made on case-by-case basis in accordance with national law. What should be taken into account in such analysis, will be discussed further in this chapter.

Another primary issue concerning Pirate Bay cases, in addition to compliance with special liability regime provided for by the eCommerce Directive, is the question of proportionality of the judgments. The administrators of The Pirate Bay took their case before the ECtHR which has recently assessed proportionality of judgment of the Svea Court of Appeal. The ECtHR considered in its final decision that the national courts had succeed in balancing the competing interests at stake, namely the right of the applicants to receive and impart information and the necessity to protect copyright, when convicting the applicants to the referred sanctions. Application was considered as manifestly ill-founded. Altogether, this may encourage and evoke copyright owners to make attempts to tackle service providers of file-sharing platforms more actively. Before conducting such kind of activity, it should be born in mind by all the parties involved to disputes concerning P2P file-sharing, that the message given by the ECtHR is not prevalence of copyright over other interests. The ruling emphasizes the meaning of balancing competing interest at stake.

5.3.2 Service provider’s criminal liability in P2P arrangements

Before going any further in assessment of criminal law matters, the attention should be directed on competence doctrine of the EU. As referred in section 3.3.2 concerning public law enforcement, substantive criminal law is mainly under competence of the Member States. That means that as a principle EU law cannot interfere so much to the assessment of intermediaries’ criminal liability. Therefore this thesis cannot define how the criminal liability should be assessed in light of EU law. Instead, in order to understand the referred cases and problems concerning service providers in P2P networks, this section points out few important aspects that should be taken into consideration in any case concerning liability of an intermediary.

As referred above, in modern P2P arrangements the principal offence — preparing copy of a work and sharing it — is conducted by a user of the network since an actual sharing is

---

235 Edwards 2009 p. 79.
236 Neij and Sunde Kolmisoppi v. Sweden no. 40397/12 [2013].
237 See Frabboni 2010 p. 141—142.
conducted between users’ computers. The role of service provider may be necessary and / or active part of the offence by providing searching tools and managing the traffic. It should be highlighted that this is not always the case since P2P arrangements are not based on one single model. On the side of copyright holder the question is on whom the claims of copyright infringements can be directed. In centralised arrangements interference to the activities of the service provider may be considered as the most effective way since the arrangement relies on functions provided via the central server. On the other hand, termination of the activities of a service provider may just make the users to conduct their activities via services of another provider. If P2P arrangement does not include any centralised service the situation gets more complicated than in centralised arrangements. Since in such a case there are no any middlemen, the only option is to direct claims on individual users if national law provides such an option. However, directing claims on individual user is completely another topic that falls outside of the scope this thesis and therefore is not reviewed further in this context.

In Swedish and Finnish criminal cases concerning copyright infringements committed by using P2P networks, the provider’s liability have been approached by complicity doctrine in accordance with applicable criminal laws. As an example, complicity doctrine was applied in referred Swedish Pirate Bay case by the Svea Court of Appeal in which the administrators of the file-sharing service were held abettors to the principal offence. According to Finnish criminal law it has been considered in legal literature that usually an intermediary cannot be held liable for principal offence but complicity to the principal offence may apply. As a principle, in Finnish criminal law any form of complicity may therefore be applicable. Still, applicability of complicity doctrine should be approached with carefulness. According to Sorvari liability of intermediary for a copyright infringement, in accordance with complicity doctrine, is applicable only exceptionally.

As a comparison to the case law of US, which is one source of inspiration especially in European telecom and technology field, complicity interpretation does not differ so much from contributory and vicarious liability applied in US file-sharing cases. In Aimster it was

---

238 See Vierto 2007 p.181. It should be noted that copyright infringements may be examined through civil proceedings as well. Moreover, complicity doctrine is applicable only in case the applicable law in question allows such interpretation.

239 Compare to the interpretation of the Finnish Supreme Court in KKO 2010:47 Finreactor in which the court considered some of the administrators of the P2P network liable of copyright infringements as offenders.


242 In the context of net neutrality discussion the Commission has stated that it follows international developments closely and will continue to take them into account in its own thinking on possible approaches. COM(2011) 222 final p. 8.
held that because of impracticability or futility for a copyright owner to sue a multitude of individual infringers, instead a copyright holder can sue a contributor to the infringement as an aider and abettor. In *Grokster* the requirements for contributory liability were a direct infringement of a primary infringer, an offender’s (here a service provider’s) knowledge of the infringement and a material contribution by an offender to it. Vicarious liability requires an infringer receiving some financial benefit by having some direct or indirect relation to the infringing conduct and that an infringer has the right and ability to supervise the primary infringers.

Applying of the complicity doctrine includes several problems. Applying criminal law provisions to a modern online environment may be problematic because of conceptual difficulties. For example, in Finland the complicity doctrine is designed for traditional offline environment which makes applying it to the P2P problematic in many ways. Moreover, legal uncertainty steams from the fact that criminal law is a very national field where national tradition dominates. Complicity doctrine is interpreted differently in different Member States. In addition to this, as stated before, P2P arrangements are not illegal itself. Therefore, illegality of the activities pursued by a service provider should be reviewed carefully in each individual case in accordance with rule of law principle by taking into account purpose and actual use of a service or an arrangement and each provider’s awareness and level of activity in contributing infringements.

### 5.4 Applicability of the special liability regime to P2P arrangements

A service may fall outside of the coverage of special liability regime if it does not fulfill the nominal requirements for applicability of the eCommerce Directive. As referred before in chapter 2, the eCommerce Directive applies to information society services. For example, P2P arrangements may not be intended for economic purposes and therefore fall outside of the special liability regime already at this point. Secondly, it should be reviewed whether the service is covered by nominal requirements based on Articles 12—14.

P2P arrangements tend to serve different than mere economical purposes. Heavy reliance on looking at what financial gain an intermediary makes has led to case-by-case assessment of

---

243 **In re: Aimster Copyright Litigation** 334 F.3d 643 [2003].
244 *MGM v. Grokster* 380 F.3d 1154 [2004].
245 WIPO workshop keynote paper Online Intermediaries and Liability for Copyright Infringement p. 35.
247 Information society service, in the meaning of the eCommerce Directive, is defined in the directive 98/34 as amended by the directive 98/48. See further chapter 2.
the special liability regime, which may enhance legal uncertainty for intermediaries.\textsuperscript{248} As referred in this thesis, remuneration requirement may be fulfilled by indirect economic benefits e.g. from advertisements\textsuperscript{249}. Such an interpretation is justified since dominant modern models of electronic business are based on making economic benefits by lateral ways in relation to the major service offered\textsuperscript{250}. However, there are online services in the market which do not serve economic purposes. Should such services fall outside of the special liability regime? The definition of information society service in the context of the eCommerce Directive seems to fit poorly to the reality of the markets since the eCommerce Directive is promoting namely electronic commerce, i.e. economic activities. However, the EU is not considered as just an economic union, but it has nowadays different functions as well. According to Article 3(3) TEU the EU establishes an internal market to contribute economic and social progress, but also to promote \textit{inter alia} scientific and technological advance. One may get into conclusion that by broadening coverage of liability restriction to services with no economic purposes as well the EU could actually promote technical innovations which are made, not just by employees of companies, but also by normal users of the Internet with advanced skills in IT-technology. Such innovations may have positive impact to the economy indirect way.

As mentioned before, P2P arrangements are not based on one single model and therefore compatibility with Articles 12—14 must be assessed in each case separately. These articles of the eCommerce Directive are binding in assessment of civil liability through national provisions implementing them, or in case implementation have been neglected, through direct effect doctrine\textsuperscript{251}. Even though the eCommerce Directive does not intend to harmonise national criminal laws\textsuperscript{252} it is applicable in criminal matters as well. However, the eCommerce Directive cannot have binding effect to material national criminal law or interpretation of national courts in criminal cases since the directive is not such directive meant in Article 83 TFEU by which the EU could harmonise certain aspects of criminal laws. This is connected to the rule of law principle, which is emphasized in criminal law, according to which wording of provision limits the interpretation. Another question is how the Member State has implemented the directive. A Member State may have taken Articles 12—14 into account in criminal law especially because of many early commentaries recommended to do

\begin{flushleft}
\textsuperscript{248} Edwards 2009 p. 87.  \\
\textsuperscript{249} See chapter 2.  \\
\textsuperscript{250} See Edwards 2009 p. 63.  \\
\textsuperscript{251} See section 1.2.  \\
\textsuperscript{252} Recital 8 of the eCommerce Directive. 
\end{flushleft}
so\textsuperscript{253}. The directive may have indirect effect on criminal case through principle of mutual recognition of foreign judgments if the court deciding the case takes foreign judgments into consideration, as the Finnish court did when it decided the case concerning blocking access to The Pirate Bay sites\textsuperscript{254}. At this background, it is still obvious the directive has more effect as source of law in assessment of civil liability.

Services connected to P2P arrangements are most likely considered as hosting services since the service consists of hosting of certain data. As referred above, the modern P2P search and tracking services usually do not host the shared content itself but only the files that enable users to download the shared content.\textsuperscript{255} In other words, the service may concern linking as it is common among modern online services. In that case an actual illegal content, e.g. music file including unauthorized copy of protected content, is not stored by the service. In Finnish case law hosting of Torrent files has been considered being hosting activities in the meaning of Article 14 of the eCommerce Directive.\textsuperscript{256} Despite such interpretation, it cannot be considered clear whether linking is hosting as such. Since the P2P search and tracing services fits ill to the definition of a hosting service, could they be instead considered as a mere conduit or caching services? In the EU there is no any direct answer to this question available\textsuperscript{257}. In theory there is no any obstacle for such interpretation if the conditions set out in Articles 12 or 13 of the eCommerce Directive are met in individual case. To be covered by Articles 12 and 13, it is required to remain neutral and passive in relation to transmitted content. As providing access to a communications network, P2P networks could fit into the coverage of Article 12 since ‘communications network’ is not defined precisely in the directive\textsuperscript{258}. However based on Google France and Google ruling, in order to benefit of the special liability regime the service provider should remain neutral. According to the ECJ this concerns all intermediary services, including hosting services.\textsuperscript{259} Modern online services connected to P2P tend to lack the required neutrality\textsuperscript{260}.

\begin{thebibliography}{99}
\bibitem{} See section 2.2.2.2.
\bibitem{} Helsingin hovioikeus 383, S 12/1850, 8 February 2013.
\bibitem{} See Smith 2007 p. 9.
\bibitem{} In Finreactor (KKO 2010:47) the service in question connected to file-sharing network was considered nominally being under coverage of hosting services.
\bibitem{} The US is a lot ahead in its case law in this field. See WIPO workshop keynote paper Online Intermediaries and Liability for Copyright Infringement p. 36—44.
\bibitem{} See section 2.2.1.
\bibitem{} According to Frabboni the lack of neutrality represents a main weakness in services regarding to P2P networks, like Kazaa and The Pirate Bay (Frabboni 2010 p. 144).
\end{thebibliography}
Moreover, arrangements designed or intended for illegal purposes are excluded from coverage of the liability restriction. Pursuant to recital 44 of the eCommerce Directive “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”. At this background, a service provider cannot plead to the liability restriction provided for by eCommerce Directive if the service consisting of mere conduit or caching is designed or intended for illegal purposes or if a service provider deliberately contributes illegal activities. Collaboration between a service provider and a user to pursue illegal activities constitutes awareness of illegal activities in hosting since pursuing such activities prerequisite knowledge of the storage of illegal content without removing or blocking the content. Therefore, illegal intentions a hosting provider cannot be protected by the special liability regime either.

So which activities may be considered as collaborating with user in order to undertake illegal acts? Should the evaluation be based on acts that can be objectively assessed or in pure intention? In practice combination of awareness of violations and upkeeping activities have been together considered constituting evidence of deliberate collaboration to infringing act and therefore constituting liability.

In Swedish Pirate Bay case the court considered that in order to find liability, it should be shown that the administrators acted deliberately, not only in respect to their role of facilitators but also in respect of the principal offence. In Finreactor the Finnish Supreme Court considered the liability restriction based on the eCommerce Directive being precluded because of the administrators of the file-sharing network were held being aware of copyright infringements and engaged to copyright violations by upkeeping activities and therefore liable as offenders and abettors.

Some studies suggest that principles based on the eCommerce Directive would apply in the assessment of service provider’s liability even though the service would not be covered by the said provisions. According to such interpretation principles regarding assessing awareness and activeness of a service provider, like neutrality principle and diligent economic operator

---

262 Frabboni 2010 p. 143.
interpretation, would apply. That would mean that awareness and activeness of the service provider would be in relation to the provider’s level of complicity and liability.265

However, if a service does not fall within coverage of the concerning directive a national court cannot be bounded to the interpretation of the ECJ in relation to the concerning directive. Despite of that, in general, there are no obstacles to apply principles of EU law as a source of interpretation when a national court is using its margin of appreciation, especially if such principles are established in national legal system. General applicability of principles stemming from the eCommerce Directive would be acceptable based on recital 41 of the directive according to which the directive establishes principles upon which industry agreements and standards can be based. Even though wide utilising of the ECJ’s interpretations in national courts may contribute legal certainty to the certain point in national level, taking advantage of the ECJ interpretations outside of the scope of directives does not contribute legal certainty in European point of view since all the Member States are bound by such interpretations.

5.5 Evaluation

Based on the referred case law, there are three points which have been highlighted regarding copyright cases: P2P networks as such are not illegal arrangements but P2P networks may be used for illegal file-sharing or they may be intended for illegal file-sharing.

Firstly, it should be born in mind that none of above-mentioned circumstances leads to criminal or civil liability per se. They represent hypotheses which may help phrasing of questions in examining alleged copyright infringements by providing guidance of applicability of the liability restriction provided for by the eCommerce Directive. Liability should be evaluated based on applicable national substantive law which is in conformity with EU law. In the two latter-mentioned circumstances, where networks may be used or intended for illegal file-sharing, the eCommerce Directive provides some guidance for interpretation, even directly if the directive is not implemented or applied correctly in national law. In case an arrangement is, when considered as a whole, intended for illegal purposes its provider falls outside of scope of the liability restriction provided for by the directive since according to recital 44 of the directive deliberate collaborating with users in order to share material unlawfully falls outside of the liability restriction. If the service is not considered intended for illegal file-sharing but the service is used for illegal purposes by its users the provider may

265 See Vierto p. 195.
benefit from liability shield if the activity of the provider is in compliance with circumstances provided for by Articles 12—14.

Despite the simple model set out above, there is critique to give in the current state of European electronic commerce law in respect of P2P arrangements. In the light of several legal studies and remarks regarding national case laws of the Member States, the liability restriction provisions of the eCommerce Directive seems to fit ill with services connected to modern P2P file-sharing. Therefore national courts or authorities do not receive much help from harmonised provisions and tend to solve the liability question based on differing interpretations which are made on the basis of national criminal and intellectual property laws. In prevailing circumstances different actors have wide range of approaches to choose from depending on what is the interest they aim to protect\textsuperscript{266}. This makes conducting of international online business based on modern technology more difficult by enhancing legal uncertainty that stems from conflicting interpretations and fragmented case law. Undoubtedly, there is need for further efforts to clarify the situation of providers offering P2P related services in the common market and updating the eCommerce Directive to meet reality of modern technology. Moreover, further guidance from the ECJ and other EU organs would be warmly welcomed.

What comes to balancing different interests at stake in P2P cases, as well as in cases of other online services, the appropriate balance should be found in each individual case.\textsuperscript{267} Because of this, not only the legislation should adapt to technological development but also the online services in the market should adapt to the reality of current legal and other circumstances by facing the risks that have occurred in our online environment.

\section*{6 Conclusions}

\subsection*{6.1 Definitions of intermediary services should be understood broadly}

There are two general approaches towards intermediary online services: 1) qualifying a single service as a whole whether being covered by, or outside of, the scope of Articles 12—14, or 2) subdivision of a single service into several distinct activities and applying the special liability regime only on concerning activities. The ECJ’s approach in \textit{L’Oréal and others v. eBay} was similar than the former approach of these two and Advocate General Jääskinen’s

\textsuperscript{266} In addition to this, undesirable forum shopping has been noted for example in defamation cases (Edwards 2009 p. 57—58).

\textsuperscript{267} See Frabboni 2010 p. 145.
approach in the same case promoted the latter. The subdivision approach would increase utility of the special liability regime by broadening the coverage of the provisions but, so far, it is not confirmed by the ECJ.

In general, narrow interpretation of Article 14 as well as other articles of the eCommerce Directive should be avoided. Definitions provided for by Articles 12—14 should be flexible in order to be applicable in dynamic technological environment and promote technological advance in the internal market as aimed by Article 3(3) TEU. Moreover, narrow interpretation would limit utility of the provisions and therefore hinder reaching the aims of the directive, namely free movement of information society services based on Article 56 TFEU and promoting freedom of expression protected by Article 11 of the Charter. One example of narrow interpretation applied by the ECJ regards assessing hosting services through neutrality principle by limiting liability restriction merely to technical and passive processing of the content. Instead of applying such a principle, more expedient result would be achieved when activeness of a service provider is assessed as whole. This seems to be justified based on the wording of Article 14. By following the same line, since we do not have applicable harmonised notification procedure, awareness or knowledge of illegal content should not be interpreted being connected only to certain procedures but as covering every situation in which the provider concerned becomes aware of such facts or circumstances.268

To sum up all the developments concerning interpretation of Article 14 of the eCommerce Directive reviewed in the thesis, the evaluation of regarding definition of a hosting service should be based on following conditions: 1) a service in question is considered as information society service in the meaning of directive 98/34 as amended; 2) a service should consist of storage, wholly or partly; and 3) a service provider does not play an active role of such to give it knowledge of, or control over, the data stored. In order to enjoy liability restriction it is required additionally that 4) if the provider has got aware of storage of illegal content otherwise, for example by its own investigation, claims of damages or sufficient notification, the provider expeditiously removes or disables access to such content.

In accordance with L’Oréal and others v. eBay ruling, diligent economic operator principle completes the last condition set out above. An intermediary service provider should base the decision to remove or disable access to content on whether a diligent provider would evaluate content being illegal. In light of other case law of the ECJ, evaluation includes obligation to

268 C-324/09 L’Oréal and others v. eBay [2011] paragraph 121.
take appropriate measures, as far as it is reasonable, to solve the question and assess consequences of action and passivity.\textsuperscript{269}

6.2 Injunctions imposed on service providers must be proportional

In order to avoid unjust burdens to businesses of online service providers, the general monitoring ban, provided for by Article 15 of the eCommerce Directive and confirmed by the ECJ, should be considered absolute. Specific monitoring measures are not covered by the ban and therefore they may be imposed on service provider in accordance with national law in specific cases\textsuperscript{270} in accordance with principle of proportionality, i.e. when prescribed by national law, measure is necessary to the legitimate aim and different interests at stake are balanced. The general monitoring ban, when understood correctly, serves well its purpose to hinder preventive censoring of contents in online services. The ban cannot be strictly restricted to those services which fulfill definitions of mere conduit, caching and hosting services since the ban serves basic values protected in the legal system of the EU. According to Article 3(3) TEU the EU aims to contribute economic growth, employment and social progress in the internal market. The eCommerce Directive is aimed to ensure proper functioning of the internal market and especially free movement of information society services based on Article 56 TFEU. Moreover, undue burdens to conducting business are not acceptable taking into account Article 16 of the Charter which has the same value than the Treaty provisions. The ECJ has considered Article 15 of the eCommerce Directive together with other applicable provisions concerning injunctions, especially Article 3 of the Enforcement Directive, by taking such an approach according to which the ban serves values having primary nature, as fundamental rights\textsuperscript{271}. The general monitoring ban is justified since it is difficult to imagine such a general injunction that could be considered proportional taking into account different interests. There are several reasons for this. Firstly, monitoring all the stored or transmitted data would, taking into account state of art of technology, require such resources that especially small and middle-sized companies would probably not be able to cover. Such a burden is not acceptable in light of primary legislation of the EU, especially the said Article 3(3) TEU. Another reason to justify general monitoring ban regards to balancing different interests. According to the rule theory referred in this thesis a right include obligation to respect rights of others. A right owner, who assumes his / her rights been

\textsuperscript{269} See section 2.2.3.
\textsuperscript{270} Recital 47 of the eCommerce Directive.
\textsuperscript{271} Such an approach was taken for example in C-275/06 Promusicae [2008] and C-360/10 SABAM v. Netlog [2012].
violated by using an online service, must respect rights of a service provider that provides the service. Monitoring obligation of non-specified content would not meet requirements of a fair balance between interests, i.e. obligation to respect rights of service providers, users and intellectual property right owners simultaneously²⁷².

Balancing of interests must be performed by virtue of the principle of proportionality. Rights to be reconciled are freedoms protected by the Charter, which has the same legal value than the Treaties²⁷³, namely freedom to conduct business (Article 16), freedom of expression (Article 11), right to intellectual property (Article 17(2)) and protection of personal data (Article 8). The directives and other provisions of EU law as well as rulings of the ECJ provide guidance of how the reconciling should be actualised. Despite the special role of freedom of expression in western democratic information society, it cannot be considered having prevalence over right to intellectual property, freedom to conduct business or protection of personal data in accordance with EU human rights law. Same “rule” concerns intellectual property rights. The development of European human right law does not illustrate any victory of intellectual property right but the significance of rightful balancing of different interests. In each case the interests at stake must be balanced based on applicable national law in conformity with EU law and taking into account engagement to the ECHR. Duly justification and proportionality of decisions and judgments is essential when several rights are reconciled in order to reach a fair and admissible conclusion.

Injunctions that are imposed in order to enforce intellectual property rights must be fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays²⁷⁴. Techniques though which illegal content can be prevented varies. None of the techniques (by general means as blocking, filtering etc.) is illegal or precluded per se but the way techniques are used may be precluded in light of EU law as not being proportional. Since an injunction restricts activities of an intermediary service provider, an injunction should be feasible in order to fulfill requirement of fair balance between interests. As it has become evident, approach towards general blocking attempts is reserved, and it should be. One may get into the conclusion that the more general the action is (blocking or disabling access to certain content) the more careful the court or other national authority must be with balancing interests by virtue or principle of proportionality and deciding of an injunction.

²⁷² See Montero Van Enis 2011 p. 27.
²⁷³ Article 6(1) TEU.
²⁷⁴ Article 3(1) of the Enforcement Directive.
6.3 De lege ferenda, position of intermediary service providers requires revision

Currently, assessment of intermediary liability is based on case-by-case analysis and national case laws are fragmented. These facts are likely to increase legal uncertainty and effect negative way on the development in the common market. As Frabboni has suggested, contributing taking on superior business models could be enhanced if uncertainty over the legal framework in which intermediaries operate is reduced, not just in national but also through a regional approach.275

The Commission has considered in its communication report in 2012 that “consultations and analyses carried out indicate that a revision of the [eCommerce] Directive is not required at this stage”. Instead the Commission considers necessary to improve the implementation of the directive and provide clarification concerning the liability of intermediary Internet providers.276 Clarification is without a doubt needed, but based on the thesis in hand, it sounds humorous to consider that clarifying would cause any major difference. Revision of the provisions concerning the intermediary service providers’ special liability regime is needed since only very few provider of modern online services based on user-generated content may benefit from the regime because Articles 12—14 rarely apply to the said modern services. As far as the regime applies only in very few cases, the trend is to evade it by choosing such an interpretation which excludes application of the regime.277 Moreover, the former study SMART 2007/0037 commissioned by the Commission's Information Society and Media Directorate-General explicitly recommends enlarging and clarifying the scope of the special liability regime. The recommendation of the study is following:

“The current special liability regime set forth by the eCommerce Directive is too focused on three types of services (mere conduit, caching and hosting), and is too dependent on particular technologies. As a result, many new (Web 2.0 and cloud computing) services are not protected against third party liability. The special liability regime should therefore be revised to protect all online third party information processors against liability claims, excluding service providers that induce their users to infringe third party rights.”278

275 Frabboni 2010 p. 145—146.
How about the ECJ? It is clear that the ECJ plays important role in EU legal system because of its evolutionary character. Evolutionary character is an inevitable consequence of preliminary ruling procedure provided for by Article 267 TFEU since the assignment of the ECJ is to give rulings of how the Treaties and secondary legislation of the EU should be interpreted by the Member States. However, the ECJ has had many opportunities to clarify interpretation of the eCommerce Directive, but it has relied on timorous policy by giving guidelines and interpreting definitions broadly. Such an approach is understandable taking into consideration an interest to keep definitions flexible for new technological innovations within the EU. Moreover, it is a fact that our technological environment is getting very complicated. Such an extended expertise in technological field, which is required in order to understand modern online services, is usually not available for courts. This may cause prudence and reluctance to commit on technological questions. Certain level of prudence is justifiable since erroneous impression may lead to unreasonable results especially when the Member States are bound to interpretations of the ECJ when applying EU law through preliminary ruling procedure provided for by Article 267 TFEU. On these grounds it seems probable that, even though the ECJ rulings may clarify the interpretations in future, these rulings do not solve the issue that many modern online intermediaries remain outside of the coverage of the liability shield, and that may evoke measures that are likely to breach freedom of expression and reduce legal certainty in the common market.

As became clear in chapter 5, services connected to P2P networks fit ill to the coverage of intermediary services defined in Articles 12—14 of the eCommerce Directive. In modern P2P arrangements, service providers do not usually store or transmit illegal material directly on, or via, their servers and therefore such service providers cannot plead to the liability restriction even though they would pursue activities by having intermediary role in respect to the content. Moreover, how should be assessed services which are not provided for remuneration and therefore would not be considered as information society services in the meaning of the directive 98/34 as amended? Moreover, for example notification procedures would be, based on phrasing of the eCommerce Directive, applicable to hosting services and to certain point to

279 Evolutive character of EU law stems from preliminary ruling procedure provided for by TFEU. Therefore evolutive theory is in conformity with modern positivistic theory. For example Senden has argued for evolutionary character of the ECJ (Senden 2011 p. 169—171).

280 For example Van Eecke notes that in L’Oréal and others v. eBay the ECJ failed to provide any further guidance instead of stating that notification by a third party must be sufficiently precise and adequately substantiated (Van Eecke 2011 p. 1485). In L’Oréal and others v. eBay the ECJ interpreted awareness of service provider broadly “covering every situation in which the provider concerned becomes aware, in one way or another, of such facts or circumstances” (C-324/09 L’Oréal and others v. eBay [2011] paragraph 121).
As far as a service falls outside of the definitions of these services, it is unclear how a given notification of alleged illegal content should be approached. Would the notification anyway set out an obligation to the service provider to take measures in order to prevent illegal activity pursued by its users with help of the service? And which are the consequences of passivity? The line of questions goes on and on.

P2P arrangements is just one example of web 2.0 based technology which fits ill with provisions of the eCommerce Directive and which illustrates need for revision of the provisions. The eCommerce Directive's special liability regime for online intermediaries has been considered focused on Web 1.0 services, leaving new service models, particularly the most promising Web 2.0 and cloud computing services, unprotected. As pointed out before, linking to the content locating in another service or other location has aroused legal questions which still remain unsolved. Which factors make linking constituting liability if the content behind the link appears to be unlawful? This and other similar issues illustrates the need for further attempts to revise the law to respond needs of, and be applicable to, modern online environment. It is apparent, that just a clarification of interpretation may cope only small range of the problems occurred.

The initiative of the Commission for harmonised N&A procedure may contribute development towards legal certainty presuming that there will be proper outcome. NTD procedures are in general considered as potential solutions since they clarify the requirements set out by Articles 13(1)(e) and 14(1)(b) concerning removing or disabling access to illegal information, and therefore clarify applicability of the special liability regime. Such development could, depending on the outcome, clarify assessment of unlawfulness of the material alleged illegal, improve service provider’s position by clarifying consequences of actions and passivity etc. However, at the moment of finishing the thesis in hand, there were no any sign of developments in this matter.

In order to improve legal certainty in international online environment, development of legal framework should be contributed by international actors. As stated by the Commission, Europe should stay in the frontline of development and provide the best possible environment for electronic commerce. In order to reach these aims there should be adequate platform where service providers may utilise technical innovations and create more of such. The common framework of the EU is expedient forum for developing legislative environment for

281 Article 13(1)(e) and 14(1)(b) of the eCommerce Directive.
online business. That is why different actors of the EU, especially the Commission, should for the sake of legal certainty take seriously the need for revision of coverage of the special liability regime of the eCommerce Directive as pointed out by the study referred above. Edwards has expressed the need for harmonisation by pointing out that “any future [EU] legislative regime might well be best expressed in more detailed terms, and as maximum harmonization, both to produce more predictability for businesses operating across the Single Market”283.

If we have to choose between clarifying interpretation of prevailing provisions and revising the special liability regime, the latter would definitely contribute aims behind the eCommerce Directive and legal certainty more than the former option.

6.4 Openness of the Internet policy – how to steer a ship in a storm?

In the beginning of this thesis was quoted the beautiful words of the Commission of “continuous process to ensure that Europe stays in the frontline of development and provides the best possible environment for e-commerce with a maximum level of legal certainty both for business and consumers whilst ensuring a minimum of burdens for business and Member States”. If the EU avoids revising of relevant provisions, could the openness of the Internet policy be utilised in respect of these aims?

The change in the market has required introducing new policies. The openness of the Internet is one of such policies in the European electronic communication field.284 Openness of the Internet aims to the same targets as the net neutrality policy: contributing users’ ability to access and distribute information or run applications and services of their choice as well as transparency of offered services in common telecom framework285. It is actually a reflection of freedom of expression and its meaning to European online service providers is still under discussion. The core of net neutrality debate actually addresses the issue of whether online service providers should be allowed to manage the traffic flowing through their networks or, on the contrary, whether they have to treat all bytes on an equal basis286. However, it is predictable that openness of the Internet, as considered a little more broad perspective, will be more and more important policy objective and will effect in other entities outside the question

283 Edwards 2009 p. 87.
284 See e.g. the Council of Europe recommendation CM/Rec(2011)8 on the protection and promotion of the universality, integrity and openness of the Internet.
285 See section 3.6.
286 Laguna de Paz 2010 p. 1968.
of traffic management as well, since blocking of services which store user generated content as well as other restrictive measures have aroused some concern of the threat of censoring the Internet.  

In addition to emphasizing importance of the open character of the Internet, it is important that different actors understand why certain measures restricting the openness of the Internet are necessary. In this regard, considerations based on analogy should be abandoned and weight should be directed on duly justification of reconciling different interests in question. In other words, those who any restrictive measure concern, including users of a blocked service, should be well informed why the measure is necessary, proportional and serving legitimate aim. The case-by-case assessment may be difficult to predict by intermediaries but since the role of intermediaries is as messy as it is at this moment, do we have any other choice than rely on case-by-case analysis and stand certain level of unpredictability until better solutions will occur?

The metaphor in the headline of this section illustrates overall phenomenon in Europe in Web 2.0 era where the EU, as a ship in a storm, tries to contribute its policies while opposing sides are more and more far from each other and trying to contribute interpretations and diverging new policies that fits to their interests. A ‘storm’, as the prevailing situation has been called in legal literature regarding to role of intermediaries, is a felicitous expression of what is going on at the moment. The counterpoints may be for example a copyright owner and a service provider, or an access provider and an average user of the Internet – interests are diverse. Whatever the confrontation is, openness of the Internet policy could contribute fairness since any extreme options are avoided and transparency and competition in the market emphasized. These points have been already acknowledged in the EU thus the question is how to make different actors contribute them. In other words, how to steer the ship in this storm?

287 According to recommendation CM/Rec(2011)8 (paragraph 7) of the Committee of Ministers “the protection of freedom of expression and access to information on the Internet and the promotion of the public service value of the Internet are part of a larger set of concerns about how to ensure the universality, integrity and openness of the Internet”.

288 See Edwards 2009 p. 87.

289 See Marsden 2009.