Conquering Copyright:
Viable E-Business Models for Media ISPs

Tuulikki Haaranen

Department of Accounting and Commercial Law
HANKEN School of Economics
Helsinki
2013
Abstract:

This thesis is written for future media entrepreneurs. The aim is to improve entrepreneurs’ understanding of how copyright influences the development of online media businesses and services. The thesis looks for answers to two questions: What kinds of online media services are legitimate on the basis of current statutory and case law in copyright and what kinds of e-business models are viable for media Internet service providers (ISPs).

The study examines the legality of business models of news aggregators, file hosting service providers and online video recording service providers. Legal risks involved in hyperlinking and framing, client-server and peer-to-peer platforms as well as cloud technologies are investigated.

The findings suggest that media ISPs have an increased risk of infringing copyright laws. Primarily, copyright liability for a media ISP emerges when service users communicate unauthorised content to the public and the ISP fails to remove the infringing content or hyperlinks and URLs leading to that content. ISP liability can also result from the facilitation of content and data exchange between service users if the exchanged content is used without permission. Also, the use of hyperlinks and URLs to third party websites can trigger copyright liability if an ISP has not obtained permission to link third party content to its website.

The legal risks cannot be sufficiently reduced by resorting to ISP liability limitation statutes. Instead, online media entrepreneurs should from very early on to design their businesses to include a plan for how the exploitation rights to content are acquired, what service users are allowed to do on the website, what kinds of content monitoring and takedown procedures the website deploys, and what kind of a linking policy the website has.

Keywords:
copyright, ISP liability, ISP safe harbours, media entrepreneur, e-business
### ACRONYMS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BTAP</td>
<td>WIPO Beijing Treaty on Audiovisual Performances</td>
</tr>
<tr>
<td>CC</td>
<td>Creative Commons</td>
</tr>
<tr>
<td>CJEU</td>
<td>Court of Justice of the European Union</td>
</tr>
<tr>
<td>CMO</td>
<td>Collective management organisation</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain name system</td>
</tr>
<tr>
<td>DVR</td>
<td>Digital video recorder</td>
</tr>
<tr>
<td>ECL</td>
<td>Extended collective licensing/license</td>
</tr>
<tr>
<td>IP</td>
<td>Intellectual property</td>
</tr>
<tr>
<td>IPL</td>
<td>Intellectual property law</td>
</tr>
<tr>
<td>IPR</td>
<td>Intellectual property right</td>
</tr>
<tr>
<td>IPTV</td>
<td>Internet Protocol television</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet service provider</td>
</tr>
<tr>
<td>nPVR</td>
<td>Network personal video recorder</td>
</tr>
<tr>
<td>P2P</td>
<td>Peer-to-peer</td>
</tr>
<tr>
<td>TPM</td>
<td>Technical operation measure</td>
</tr>
<tr>
<td>TRIPS</td>
<td>Agreement on Trade-Related Aspects of Intellectual Property Rights</td>
</tr>
<tr>
<td>UGC</td>
<td>User generated content</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator (web address)</td>
</tr>
<tr>
<td>VCR</td>
<td>Videocassette recorder</td>
</tr>
<tr>
<td>VOD</td>
<td>Video-on-demand</td>
</tr>
<tr>
<td>WCT</td>
<td>World Intellectual Property Organisation (WIPO) Copyright Treaty</td>
</tr>
<tr>
<td>WIPO</td>
<td>World Intellectual Property Organisation</td>
</tr>
<tr>
<td>WPPT</td>
<td>World Intellectual Property Organisation (WIPO) Performance and Phonograms Treaty</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

## 1 INTRODUCTION

1.1. PURPOSE OF THE STUDY

1.2. THEORETICAL AND METHODOLOGICAL UNDERPINNINGS

1.2.1. Theoretical Foundation

1.2.2. Research Approach

1.3. DELIMITATIONS OF THE STUDY

1.4. STRUCTURE OF THE THESIS

## 2 INTRODUCTION TO COPYRIGHT

2.1. FOUNDATIONS OF COPYRIGHT

2.2. WORKS PROTECTED BY COPYRIGHT

2.3. RIGHTS PROTECTED BY COPYRIGHT

2.4. TYPES OF RIGHTS

2.5. MONETISING COPYRIGHTS

2.5.1. The Role of Collective Management Organisations

2.5.2. Creative Commons Licenses

2.6. LIMITATIONS TO COPYRIGHT

2.6.1. Fair Use In the United States

2.7. COPYRIGHT LIABILITY, SANCTIONS AND REMEDIES

2.8. LIABILITY LIMITATIONS OF INTERNET SERVICE PROVIDERS

## 3 LEGALITY OF ONLINE MEDIA SERVICES

3.1. ARE LINKING AND FRAMING ALLOWED?

3.1.1. Hyperlinking

3.1.2. Framing and Inlining

3.1.3. Conclusions

3.2. LEGITIMACY OF FILE SHARING SERVICES

3.2.1. Pre-Internet Era: Sony Betamax and Amstrad

3.2.2. Challenges of YouTube

3.2.3. Notorious P2P Services

3.2.3.1. Napster

3.2.3.2. Grokster

3.2.3.3. Kazaa

3.2.3.4. The Pirate Bay and Finreactor
1 INTRODUCTION

“Is Twitter more like a phone company or more like a newspaper?”

The question of Managing Editor Nilay Patel of The Verge may sound bizarre and even meaningless but when positioned in the context of copyright the question becomes relevant.

Every company and individual who deals with written text, photographs, music, films, television shows, radio shows, or visual arts online is affected by copyright. Copyright faces the challenge of keeping up with technological and socio-economic advancements. When new technologies emerge, our production, distribution, communication, and consumption practices are likely to change paving the way for new business models and service innovations. It takes time before legislators start to grasp the implications of the new forms of industrial and market behaviour. Consequently, the development of legislation falls behind forcing tribunals to interpret emerging business and consumer behaviour in legislative contexts that were developed for other purposes.

As there is no law that regulates Twitter as such, we need to look for the closest equivalents. If the business model of Twitter comes closest to the business models of telecommunications operators (“phone companies”), which provide access to communications networks, we could resort to statutes that regulate businesses in the telecommunications industry. If Twitter is perceived to operate more like a publishing company, provisions of freedom of speech as well as defamation and broadcasting laws might be more appropriate. Regardless of the classification of the service, copyright applies if literary or artistic works are reproduced, made available to the public, or adapted within the service.

Most of us know that Twitter is neither a phone company nor a newspaper. It is a microblogging and social networking service on the Internet enabling social interaction

---

1 Patel (2012)  
2 Cf. The Verge (2013)  
3 The scope of protection and exclusive rights afforded to rights holders are harmonised to great extent. This is due to the widely ratified international treaties and conventions such as the Berne Convention for the Protection of Literary and Artistic Works (1886), the Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (1961), Agreement on Trade-Related Aspects of Intellectual Property Rights, TRIPS (1994), WIPO Copyright Treaty, WCT (1996), and WIPO Performances and Phonograms Treaty, WPPT (1996).
and content sharing. It allows people and organisations to be in contact with one another through short written messages, photos and videos. Private citizens do not pay for the service. Twitter finances the service primarily by selling advertising space. In addition, Twitter and other social media services generate income increasingly from aggregating and selling user data to companies, which use the data in lead generation, advertising, as well as product and service development.

On Twitter, the published messages are called 'tweets'. Tweets constitute so-called user-generated content (UGC). UGC is content that service users produce and publish independently without the interference of the service provider. After a tweet has been published for the first time other users that have registered for the service can respond to the message and re-tweet (re-distribute) it. Users of Twitter control independently the circulation of their tweets. They can allow everybody using the service to view and respond to the tweets or they can limit the access and interaction to their trusted friends within the service. In deciding what to publish and re-distribute and to whom service users engage in self-regulation and possibly self-censorship.

In addition, the users must comply with Twitter's Terms of Service. In general, the terms of service of online media firms are dictated by their business objectives and by national and international legislation such as contract, e-commerce, data protection, consumer protection, copyright and trademark laws. If a Twitter user does not comply with the Terms of Service, Twitter reserves the right to “remove or refuse to distribute any content […], to suspend or terminate users, and to reclaim usernames without liability”. Together with Twitter Privacy Policy the Terms of Service also allow Twitter to disclose user-related information to third parties such as advertisers, data mining service providers and other service providers that are under confidentiality agreements. In addition, Twitter has the right to disclose user information to third parties in order to “comply with a law, regulation or legal request”.

---

4 Social networking services may impose different policies on individuals and firms. Commercial actors may be required to pay various fees in order to gain visibility. More information: Dekel (2013).
5 According to Tibken (2013), in 2012 the advertising revenue of Twitter was $583 million and it is expected to exceed $1 billion in 2015. More information: Kobie (2010).
6 Elliot (2013)
7 The IPO filing of Twitter reveals that its current data selling business is worth $47.5 million (Dwoskin 2013).
8 Cf. Twitter (2013a)
9 Id.
10 Twitter (2013b)
11 Id.
Twitter does not monitor, moderate, edit or censor UGC proactively. Should there be a breach of the Terms of Service or Privacy Policy the corrective measures are retroactive and can lead to a content removal or suspension of the user account. However, Twitter and other social networking and content sharing services have a possibility to use automated content filtering technologies to monitor and remove content that can be interpreted as offensive, abusive or spam or to identify content that might infringe copyrights. In addition, service users and third parties can report offensive behaviour of a user to the service provider. The same applies to alleged copyright infringements. If a tweet includes copyrighted content such as photos or videos, which the service user is not authorised to distribute, the rights holder has a legal right to require that the service provider removes the content from the service.

The business concept of Twitter is fairly novel. The site was first launched in summer 2006 and the business model has been under a continuous development ever since. Numerous other social networking and content sharing services such as Facebook, Google+, YouTube, and Tumblr operate in a similar manner. As with Twitter it is not always self-evident which laws should be applied in regulating these businesses. In Italy, the communications authority AGCOM has suggested that YouTube and other

12 Twitter (2013c, 2013d)
13 Twitter (2013a, 2013d)
15 Cf. Twitter (2013d)
16 For instance, YouTube uses an automated video identification technology called ContentID. More information about the functioning of ContentID can be found in EFF (n.d.) and YouTube (2013).
17 In summer 2012, Twitter suspended journalist Guy Adams’ account, because Adams had tweeted the work email address of Gary Zenkel of NBC broadcast network. NBC filed a complaint on behalf of Mr Zenkel. Twitter suspended Adams’ Twitter account on the basis of that he had violated the privacy policy of Twitter. Adams questioned Twitter’s actions, because the work email of Mr Zenkel was publically known. Adams’ account was unsuspended later with no further explanation from the part of Twitter. The case raised a question of what kind of obligations the service provider has in examining the legitimacy of third-party complaints. More information: Shapiro (2012) and Adams (2012).
18 Only the author of a copyrighted work or a third party to which the author has transferred the copyright has the exclusive right to make the work available to the public (Copyright Act 404/1961 of Finland, §2 and §27). Other users need a license to distribute the work. The rights owner or the collective rights management organisation representing the rights holder has a legal right to require a monetary fee (copyright fee) for the license (cf. ibid. §26).
19 The obligation of intermediary service providers acting as hosting services to remove infringing content as part of a notice-and-takedown procedure is codified in Article 14 of the EU Directive 2000/31/EC, Sections 15 and 20 of The Act on the Provision of Information Society Services of Finland 458/2002, and Section 512(c) of the United States Copyright Act Title 17 USC.
20 Takedown notices are commonplace in content sharing services. Many service providers publish the takedown notices they receive from rights holders. More information: Bilton (2013) and Chilling Effects Clearinghouse (2013).
21 Carlson (2011)
video sharing services should be treated as broadcasters. In an Australian defamation case, the Supreme Court ruled that despite the automated character of its search engine Google can be perceived as a publisher if it has received a letter of complaint and has failed to remove the defamatory content within reasonable time.

When a service provider is treated as a broadcaster or publisher before the law, it becomes liable for the content it distributes. It does not matter, whether end-users or in-house journalists have created the content. If a service provider is perceived more like a telecommunications operator (“phone company”), which merely provides the means to access the Internet and the content, the service provider could be exempt from publisher liability if it qualifies for the so-called ISP safe harbour provisions.

1.1. PURPOSE OF THE STUDY

I have chosen to write this thesis for business students and novice media entrepreneurs rather than for legal scholars. I hope that the study provides an easy-to-understand commentary on copyright and its ramifications to online media business development.

The study examines the legality of e-business models of news aggregators, file hosting service providers and online video recording service providers. In this context, the legal risks involved in hyperlinking and framing, client-server and peer-to-peer platforms as well as the cloud technologies of cyberlockers and nPVR service providers are investigated.

The primary purpose is to find out what kinds of e-services are legitimate in the content industries on the basis of current statutory and case law in copyright? Here, 'e-service' refers to the process of delivering a product, facility, data, information, function, or other utility to the market over the Internet. 'Content industries' are industries in which the exchange of literary works, artistic works, audio-visual works or music forms the basis for generating income directly or indirectly.

On the basis of the findings I will be able to outline e-business models that are viable for media Internet service providers (ISPs). ‘E-business model’ refers to
methods and means of conducting a business on the Internet with the objective to create value of the products and services that the business provides. ‘Media ISP’ is a firm that facilitates the production, distribution, and storing of user-generated media content or the re-use of extant media content on the Internet.

1.2. THEORETICAL AND METHODOLOGICAL UNDERPINNINGS

This thesis is primarily a pragmatic study. The main objective is to help extant and future media managers to develop e-businesses that are legitimate and viable. The underlying assumption is that business models that tribunals repeatedly have deemed illegal are too risky or infeasible.

In addition, the thesis aims to contribute to the on-going debate related to copyright reform. An evaluation of the ambiguities related to enforcing the judicial doctrines of private copying, making works available to the public, and no general obligation to monitor will be performed. In addition, the significance of ISP liability limitations to online media firms will be discussed.

1.2.1. Theoretical Foundation

This thesis subjects e-business conduct to legal analysis. As a consequence, the thesis is positioned between intellectual property law (IPL) and business studies.

World Intellectual Property Organisation (WIPO) defines intellectual property (IP) as the "creations of the mind". Examples of 'creations of the mind' are inventions, designs, literary and artistic works, as well as symbols, names and images used in commerce. Because IP is fairly easy to copy by competitors, who have not financially or otherwise invested in the creation and production of the property "there is a fear that without legal protection against copying the incentive to create intellectual

---

24 WIPO (n.d. a)
25 Id.
property will be undermined". By subjecting IP to legal protection IP becomes a legal right referred to as intellectual property right (IPR). IPRs "enable people to earn recognition or financial benefit from what they invent or create".

Two different types of primary sources are used: statutory laws enacted by legislatures and judicial opinions issued by courts (referred to as case law). The study deals primarily with EU and US copyright law and statutes regulating the liability of Internet service providers (ISPs). In the EU, ISP liability limitations are coded in a separate E-Commerce Directive. In the United States, ISP liability limitations are integrated in copyright legislation. The chosen case studies comprise court decisions from Europe, the United States, and Australia.

The secondary sources comprise green papers, academic literature, legal periodicals, and news publications. These have been used to increase the author’s understanding of statutory law and the implications of case law.

1.2.2. Research Approach

This study employs a so-called law reform research style first proposed by Harry Arthurs’ Law and Learning Report in 1983. Law reform research constitutes an applied interdisciplinary approach, where law is studied in a selected context as a socio-legal phenomenon with the aim to contribute to the development of knowledge in the domains of “professional constituency” and “research about law”. Chynoweth refers to this research style as socio-legal research.

Legal research is often conducted without an explicitly expressed methodology. This is probably due to the dominance of the so-called doctrinal legal research tradition

---

26 Landes & Posner (2003), p. 11
27 WIPO (n.d. a.)
29 Title 17 USC § 512
32 Chynoweth (2008), p. 31
practiced not only by researchers but also judges and attorneys. In doctrinal legal research, the "method is often so implicit and so tacit that many working within the legal paradigm consider that it is unnecessary to verbalise the process." In their study of legal research paradigms, Hutchinson and Duncan quote Judge Richard Posner, who in his 1988 article argues that law is "not a field with a distinctive methodology but an amalgam of applied logic, rhetoric, economics and familiarity with a specialised vocabulary and a particular body of texts, practices, and institutions".

The most commonly applied logic in legal analysis is based on deductive reasoning. In deductive reasoning, the researcher moves from a general principle to particular conclusions. A conclusion is inferred from two premises, a major and a minor premise, forming a logical argument referred to as syllogism. If the premises are true then the conclusion must be true. For instance:

**Major premise:** A person who has created a literary work is afforded an exclusive right of reproduction by Sections 1(1), 2(1), 2(2) of the Copyright Act of Finland.

**Minor premise:** This thesis is a literary work written by a person living in Finland.

**Conclusion:** On the basis of Sections 1(1), 2(1), and 2(2) of the Copyright Act of Finland the reproduction of this thesis is an exclusive right of the author of the thesis.

In this thesis, deductive reasoning is used to draw conclusions of the legitimacy of online media businesses on the basis of statutory law. Yet another approach is employed when drawing conclusions on the basis of case law. This approach is referred to as inductive reasoning.

---

33 Cf. Hutchinson & Duncan (2012)
34 Id. p. 99
36 Aldisert et al. (2007), Worster (2013)
37 Cf. Worster (2013)
38 Aldisert et al. (2007), p. 102-111
39 It is assumed here that this thesis is a copyrightable work forming an independent creation and original form of expression. See a more thorough discussion on copyrightability in Chapter 2 of this report.
In induction, general rules are formed on the basis of drawing inferences of specific observable phenomena.\textsuperscript{40} The degree to which the principles are true is based on the quality of observing the phenomena and drawing conclusions on the basis of the observations. The inductive logic works as follows:

\begin{quote}
In Finland, Sections 1(1), 2(1), 2(2) of the Copyright Act 404/1961 afford a person who has created a literary work an exclusive right to control a work by reproducing it.\textsuperscript{41}
\end{quote}

\begin{quote}
In Germany, Articles 1, 2 and 16 of the Act of Copyright and Related Rights afford authors of works in the literary domain an exclusive right of exploiting their works in material form including reproduction.\textsuperscript{42}
\end{quote}

\begin{quote}
In the United States, Sections 102 and 106(1) of Title 17 USC afford the owner of copyright of a literary work an exclusive right of reproduction of copies.\textsuperscript{43}
\end{quote}

\begin{quote}
In Australia, Section 31(1)(a)(i) of Copyright Act 1968 stipulates that in the case of a literary work copyright is an exclusive right in the act of reproducing the work in a material form.\textsuperscript{44}
\end{quote}

\begin{quote}
Therefore, reproducing a literary work is an exclusive right of the author all over the world entailing minor national variations.
\end{quote}

In order to be able to make generalisations of the observed phenomena the sample should be large enough. The required size of the sample is context-specific. If we evaluate the reliability of the conclusion of the example above, it is obvious that the conclusion is fairly audacious. There are nearly 200 countries in the world. It has been estimated that about ten of those countries do not enforce copyright laws in any form.\textsuperscript{45} This leaves us with nearly 190 countries. Is it possible to make generalisations on the basis of four cases out of the 190 cases available? The answer is “probably not”. However, it could be possible to argue that it is likely that many EU countries and countries with a historical connection to England accompanied with a western legal tradition are likely to enforce reproduction as an exclusive right.

\textsuperscript{40} Worster (2013), p. 8
\textsuperscript{41} Copyright Act of Finland 404/1961
\textsuperscript{42} The Act of Copyright and Related Rights of Germany
\textsuperscript{43} Title 17 USC
\textsuperscript{44} Copyright Act 1968 of Australia
\textsuperscript{45} Free & Legal Downloads (2009)
Luckily, in this case we can use at least two additional datasets to validate the results. First of all, by examining the functioning principles of the EU, we can conclude that all EU member states are obligated to implement the Information Society Directive, which recognises reproduction as an exclusive right. This means that 28 countries in Europe implement reproduction as an exclusive authorial right. Additionally, we could examine international copyright treaties, such as the Berne Convention, the Rome Convention, TRIPS Agreement, WCT, WPPT and BTAP, all of which recognise reproduction as an exclusive right. Signatories of these treaties are committed to implement the principles of the treaties in their laws. For instance, if the 167 signatories of the Berne Convention have implemented Article 9(1) in their national laws, it would be safe to conclude that 167 countries in the world recognize reproduction as an exclusive right of authors.

In social sciences, the method of using several research methods or datasets to validate research results is called triangulation. In this thesis, triangulation is used to achieve representativeness. By analysing European, American, and Australian court cases we have a possibility to gain more reliable information about what constitutes a legitimate online service on a global scale.

The case law for this thesis has been selected by using purposive sampling. In purposive sampling, the researcher aims to achieve representativeness or comparability. In this study, the aim of the selection has been to find cases that due to their characteristics represent a broader group of e-business models under frequent legal scrutiny. The selection has been further limited to court opinions that are accessible online free of charge. Also, the language of the court decisions has limited the selection.

47 European Union (2013)
48 WIPO (n.d. b)
49 Berne Convention 9(1) stipulates: "Authors of literary and artistic works protected by this Convention shall have the exclusive right of authorizing the reproduction of these works, in any manner or form."
50 Cf. Yeasmin & Rahman (2012)
51 Teddlie & Yu (2007)
1.3. DELIMITATIONS OF THE STUDY

Despite the fact that the study explores both national and international case law and refers to laws in Europe, the United States, and Australia the thesis does not constitute a comparative study. The wide array of case law and related doctrines are discussed in order to allow us to generalise findings.

The scope of the study has been limited to copyright and liability limitations of ISPs. The limitations are necessary to keep the length of the report reasonable. However, I will allow some leeway in the context of case law analysis. In the real world, many court cases are not purely copyright disputes but rather they can require courts to examine trademark, unfair competition, contract, and defamation laws or fundamental human rights. Further, a case that falls outside copyright as such can provide valuable information about the legitimacy of e-business models.

1.4. STRUCTURE OF THE THESIS

This chapter has described how a typical online media service functions. It has positioned the study and outlined the purpose and the research approach. In the next chapter, copyright and ISP liability limitations will be presented and explained to the extent necessary to this thesis. Chapter 3 consists of an analysis of selected court decisions. The objective is to clarify the current position of international tribunals when it comes to evaluating the legitimacy of online media services. Chapter 4 provides a summary of the research findings and advice to media entrepreneurs. In the last chapter, I will discuss the judicial complexities related to the enforcement of current copyright laws and ISP liability limitations.

A list of acronyms can be found at the beginning of this report and a list of definitions of the central concepts at the end of the report.
2 INTRODUCTION TO COPYRIGHT

2.1. FOUNDATIONS OF COPYRIGHT

Copyright is an intellectual property right (IPR). Copyright grants a rights holder a legal right to allow and prohibit other people from using her works. In other words, copyright alongside with other IPRs provides businesses and individuals with protection from competition.52

The legal theory of copyright can be divided into two schools of thought: the natural law and positive law schools.53 The natural law school is based on the work of philosopher John Locke, whose labour theory of property from the 17th century54 inspired early copyright theorists to justify the existence of copyright as an author’s natural right to benefit from the productions of her intellectual labour.55 According to the natural law theorists, copyright law exists because it is proper to recognise a property right in intellectual productions that emanate from the minds of individual authors.56

The positive law school of copyright has its origins in the 18th century Great Britain and the world’s first copyright statute, the Statute of Anne.57 Positive law theorists emphasise the role of copyright as a utilitarian societal instrument.58 The underlying assumption is that “granting authors exclusive rights will induce more creation of useful works of art,” which benefits society.59 This approach is often referred to as the utilitarian-incentive theory of copyright.60 It proposes that the value of copyright lies in its power to provide creators with an incentive to create, and that without it creators would under-produce,61 because there would be no guarantees of receiving a financial compensation for the labour put into creating works.

52 Cf. Jacob et al. (2004), p. 5
53 White & Valkonen (2006), p. 6
54 Id. p. 7
55 Cf. Bently & Sherman (2009), p. 36
56 Id. p. 35
57 White & Valkonen (2006), p. 7-8
58 Id. p. 8
59 Id. p. 16
61 Heymann (2007)
Copyright regimes in different parts of the world tend to have attributes from both schools of thought. International copyright treaties, the Berne Convention, the Rome Convention, TRIPS, WCT and WPPT, have further harmonised copyright laws. Fundamentally, the substance of copyright is the same everywhere. However, the above-mentioned ideological differences have influenced how rights and obligations are expressed in statutes and which principles are considered more important than others.

The Continental European civil law copyright is based on the French tradition of “droit d’auteur”, the right of the author, which derives from the natural law school of thought. This principle is demonstrated as a tendency to emphasise the creative efforts of an individual. For instance, the EU Information Society Directive, which is the copyright directive of the EU, grants rights to authors, performers, producers, and broadcasters of their works. Further, the European copyright law is divided into the rights of authors (droits d’auteur) and related rights (droits voisins) of performers, producers, and broadcasters, who use and develop existing authorial works in creating their performances, recordings, and transmissions. Copyright also affords economic and moral rights to authors and performers while producers and broadcasters only have economic rights.

As a comparison, common law countries such as the United Kingdom, the United States, Canada, and Australia highlight the social and organisational nature of creating works and the principle of serving the public interest. Their copyright laws emphasise the rights holders’ right to benefit economically from the production of copies of works. For instance, American copyright law protects “works of authorship”. The creators of works are referred to as “owners of copyright” regardless of whether an individual or a firm has created the work. The division of copyrights into authors’ rights and other creators’ rights is blurred or non-existent. Even though moral rights are

---

62 White & Valkonen (2006), p. 8
63 Hugenholtz (2000)
64 Cf. Directive 2001/29/EC § 2
65 Cf. WIPO (n.d. a)
66 Bently & Sherman (2009), p. 32
67 Cf. WIPO (n.d. a)
68 The United Kingdom is a common law jurisdiction but due its EU membership British copyright laws are an amalgam of civil law and common law principles.
69 Cf. Bently & Sherman (2009), p. 36, 38
70 Id. p. 32
71 Cf. 17 USC § 102(a)
72 Cf. 17 USC
codified in the U.S. Copyright Act,\textsuperscript{73} the grant of financial rewards dominates legal thought. Disputes that in Europe would be argued under the copyright provisions of moral rights are in the United States often argued under statutes regulating trademarks and unfair competition.\textsuperscript{74}

To summarise the ideological differences, it can be concluded that droit d’auteur civil law countries protect authors’ rights and grant economic and reputational benefits as an exchange for their intellectual labour. This is considered to encourage the production of cultural goods, which in return benefits society. The common law copyright protects works as commodities, the production of which must be optimised by balancing the economic interests of producers with the needs of users of works.\textsuperscript{75} This is perceived to result in the public good.

In the enforcement of copyright laws, the above-mentioned ideological differences are demonstrated in the principles that tribunals emphasise in reaching their decisions. Occasionally, the differences can result in contradictory practices between jurisdictions with regard to which new technologies and exploitation methods are considered legal. However, civil law and common law tribunals predominantly seem to end up in similar conclusions. The route to arriving at these conclusions varies.

### 2.2. WORKS PROTECTED BY COPYRIGHT

Works protected by copyright are literary, artistic, photographic, musical, dramatic, and cinematographic works, and works of applied art.\textsuperscript{76} Copyright exists also for performing artists for their public performances, broadcasters for their transmissions, producers of phonograms for their sound recordings, film producers for their audio-visual recordings, and creators of compilations and databases for their collections.\textsuperscript{77} Also, multimedia productions are protected by copyright.\textsuperscript{78} Excluded from copyright

\textsuperscript{73} See: 17 USC § 106A  
\textsuperscript{74} Rosenblatt (1998)  
\textsuperscript{75} Cf. Landes & Posner (2003)  
\textsuperscript{76} WIPO (n.d. a)  
\textsuperscript{77} Id.  
\textsuperscript{78} Id.
protection are laws, decrees, treaties, conventions, and statements of public authorities and governmental bodies.\footnote{Cf. Copyright Act 404/1961 § 9; Title 17 USC § 105}

The concept of ‘literary work’ comprises writings in any form. Examples of literary works are books, articles, blogs, poems, manuscripts, scientific reports, and lecture materials. Also, the source and object codes of computer programmes can be protected as literary works.\footnote{TRIPS § 10(1)} The most obvious forms of artistic works include drawings, paintings, sculptures, and works of architecture but also works of applied art such as illustrations, maps, plans, sketches, and three-dimensional works relative to geography, topography, or science enjoy copyright protection.\footnote{WIPO (n.d. a)} Photographic works are works expressed by photographic means.\footnote{Id.} It is noteworthy that single still images (frames) of audio-visual works can be protected as photographs or photographic works.\footnote{Id.} Musical works constitute compositions with or without lyrics.\footnote{Tuotos (2011)} Lyrics are also protected as literary works. Dramatic works refer to theatrical plays, musicals, and pantomime as well as choreographic works.\footnote{Id.} Cinematographic works constitute audio-visual works such as feature and animated films, short films, documentaries, and television programmes.

Many works assimilate several copyrights. For instance, a typical sound recording encompasses the copyright of several composers, lyricists, arrangers, and musicians as well as the copyright of the record label, which has published the sound recording. If you unlawfully distribute an album of your favourite band on the Internet, you end up violating the copyrights of all the above-mentioned rights holders. An unlawful distribution of a film on the Internet would infringe at least the copyright of the producer, director, scriptwriter, composer and actors, and possibly the copyright of the cinematographer, scenographer, costume designer, and other crewmembers if their contributions exceed the threshold of originality. Further, the copyright of the broadcaster would be violated if you have copied the film from a television channel.

Copyright protection can also be afforded to collections of literary and artistic works.\footnote{Id.} Typical collections are encyclopaedias and anthologies. Compilation albums that
feature songs from various artists are also protected by copyright. Today, collections often take a form of a database on the Internet. Compilations and databases are essentially collections of other authors' works. They are inherently derivative. A compilation or a database can be copyrightable if it is an "intellectual creation",\(^ {87}\) which by reason of the selection and arrangement of the contents\(^ {88}\) demonstrates that the compiler has made substantial investments in creating it.\(^ {89}\) Further, a database must fulfil three criteria to be copyrightable: (1) it must comprise a collection of independent materials, (2) the materials must be arranged in a systematic or methodological manner, and (3) the materials must be individually accessible.\(^ {90}\) In the Nordic countries copyright exists also for the so-called unoriginal collections in a form of catalogue protection.\(^ {91}\) Catalogue protection can be granted to catalogues, tables, almanacs, calendars, timetables and similar collections of data if their creation has required substantial resources to make.\(^ {92}\)

**Copyright protection is afforded to** works that constitute *original forms of expression*. Ideas are not copyrightable.\(^ {93}\) The unfulfilled love between a teenage girl and a teenage boy from rival families is an idea. When a film crew makes a film on the basis of this idea, the film forms an original form of expression. When a theatre group uses the idea in a theatre play, the play forms another kind of an original expression. The expressions of the film crew and the theatre group would be copyrightable even if they reminded one another. The expressions of the two artistic groups would have to be very similar before one of the works would infringe the other's copyright. Copyright law allows a fairly generous leeway in terms of similarities between expressions before an infringement occurs.

Originality means that the work must originate from the author in the meaning of not being a copy of another author’s work.\(^ {94}\) A work must be an independent creation,\(^ {95}\) which results from the author’s own intellectual labour. The ideas behind the expression do not need to be original.\(^ {96}\) A copyrightable work must also be substantial

---

87 Cf. Berne Convention § 2(5)
88 TRIPS § 10(2); WCT § 5
90 Id. p. 1120-1121
91 Cf. Olsson (1999)
92 Cf. id.
93 Cf. Title 17 USC, § 102(b)
94 Jacobs et al. (2004), p. 154
95 Cf. Copyright Act 404/1961 (Finland) § 4(2)
96 WIPO (n.d. a)
enough. It must embody enough work, labour, skill or taste. However, the merits of the work do not influence whether it is copyrightable. The paintings of a skilled painter and an inept painter are both protected by copyright. Also, unpublished and published works enjoy copyright protection.

Copyright emerges automatically. Copyright comes into being either upon the creation of the work or upon the fixation of the work into tangible form (paper, hard disk, film etc.). There is no need to apply for copyright protection. However, in some countries, such as in the United States and the United Kingdom, copyright holders can voluntarily register their works at local authorities.

2.3. RIGHTS PROTECTED BY COPYRIGHT

Copyright affords rights holders an exclusive right to control the making of copies of works, the distribution of works or copies made of them, and the making of adaptations of works.

The right to control the making of copies is referred to as the reproduction right. The reproduction right enables the rights holder to prohibit the copying of her works in whole or in part, directly or indirectly, temporarily or permanently by any means and in any form including a transfer of a work to a device with which it can be reproduced or communicated.

It is noteworthy that copyright law authorises copyright holders to prohibit reproduction also “in part”. There are no quantitative criteria for how big a portion ‘a part’ is. A single film frame, which lasts fractions of a second in a two-hour feature film, can be copyrightable as a photograph or photographic work. The use of such a frame without the permission of the author would be a copyright violation. Also, the use of a

---

97 Jacobs et al. (2004), p. 154
98 Id. p. 155
99 WIPO (n.d. a)
100 Jacobs et al. (2004), p. 153
101 Id. p. 162
102 Cf. Title 17 USC, § 102(a)
103 More information: U.S. Copyright Office (2013) and The UK Copyright Service (2013)
104 Cf. Berne Convention § 9, 12, and 17
105 Cf. Copyright Act 404/1961 (Finland) § 2(2); Directive 2001/29/EC § 2; Title 17 USC § 102(a)
bass line comprising three notes from a four-minute song could be an infringement. In copyright, snippets of works can be afforded copyright protection if they form a substantial part of the work. Unfortunately, ‘substantial part’ is not defined in copyright law. However, courts have interpreted substantial part “to mean a qualitatively significant part of a work even where this is not a large part of the work”. Therefore, even a small portion of a work can be interpreted to constitute a substantial part. In copyright, substantiality is measured in qualitative terms.

Copyright affords rights holders also an exclusive right to make available, publish, distribute, rent, lend, perform and display works to the public. The use of the concepts and the definitions of the concepts vary between jurisdictions.

The making available right constitutes any communication to the public by wire or wireless means, including the communication of works in such a way that allows the members of the public to access the works from a place and at a time individually chosen by them. The distribution right authorises the rights holder to prohibit any form of distribution of tangible works or tangible copies of works to the public by sale or other transfer of ownership. Yet another related right is the rental right, which allows rights holders to authorise the commercial rental of works or copies of works. The lending right grants the rights holders a right to control the non-commercial lending of works to the public. In the United States, the above-mentioned rights are referred to as the publication right and public performance right. Combined these rights allow the rights holder to prohibit the communication, publication, broadcasting, transmission, retransmission, streaming, distribution, sales, rental, lending, import, export, performance, and display of her work in circumstances, where a ‘public’ is present or expected to be present.

Copyright law does not define, what is meant with ‘public’. Courts have perceived ‘public performance’ to take place when one cannot predict who is going to see or hear the performance. In other words, making available, distribution, rental or lending to
the public occurs when the audience is indeterminate. Further, a prerequisite for a public performance is that individuals are free to access the performance free of charge or by paying for the performance. The amount of viewers is irrelevant. What matters is that the performance is offered for viewing in a space (physical or virtual) that is open for anyone to enter. In this approach, the concept of 'public performance’ excludes performance spaces in which the audience constitutes a ‘definite unit’ and a ‘closed circle’. A closed circle typically consists of family members and closest friends who have personal ties with one another. However, the nature and the circumstances of the performance influence whether the gathering of family members and friends can be considered to form a closed circle. For instance, posting a music video on Facebook to one’s 200 friends and acquaintances can hardly be considered as a private activity in a closed circle. Further, if every friend in your Facebook circle and their friends distributed the video, its audience would very quickly expand to tens of thousands of people. This would constitute an indeterminate audience.

Copyright also affords an adaptation right. The adaptation right allows a rights holder to prevent others from translating, versioning, arranging, altering, and modifying her work and converting her work into another art or technical form. An adaptation occurs, for instance, when an Italian book is translated into Danish, a theatre play is converted into a film, and a musical work is re-orchestrated or remixed. Also, the conversion of a code of a computer programme into another computer language constitutes an adaptation. Adapted works are in copyright referred to as derivative works. Derivative works are in essence new versions of extant works. Authors of derivative works have a copyright to their adaptations if they have acquired permission to adapt the original work. Authors of derivative works are further bound to exploit their works in a manner that does not infringe the rights of original authors.

115 Bently & Sherman (2009), p. 152
116 Karo (2002), p. 6
117 Id.
118 Cf. id. p. 6-8
119 Id.
120 Cf. WIPO (n.d. a)
122 Cf. Copyright Act 404/1961 § 4(1); 17 USC § 103(a)
123 Cf. Id.; Id.
Copyright holders can enforce their rights for the duration of copyright. The term of protection varies depending on the type of the work, when the work was created,\textsuperscript{124} and where it was created. In the EU, the author’s copyright currently lasts for the life of the author plus 70 years from the end of the year of her death.\textsuperscript{125} After her death her inheritors control the use of her works. In practical terms this could mean that if an author creates a work when she is 20 years old and if she dies at the age of 80, the work would be copyright protected for 130 years. The same applies for the protection of cinematographic works. The copyright protection of cinematographic works as authorial works expires 70 years after the death of the last surviving author.\textsuperscript{126} Note however that the copyright term of film producers, whose copyrights are embedded in the fixations of films ("master tapes"), lasts 50 years from the fixation or the publication of the film, whichever comes first.\textsuperscript{127} Also, broadcasters’ copyright to their transmissions lasts 50 years from the first transmission.\textsuperscript{128} According to the most recent amendments, the protection of sound recordings and musicians’ rights embedded in those recordings lasts for 70 years from the date of the first publication or the first communication to the public depending whichever occurs first.\textsuperscript{129} When copyright expires the work is passed into the public domain. Works in the public domain can be used without permission from the original authors or their beneficiaries.

\section*{2.4. TYPES OF RIGHTS}

The rights afforded by copyright can further be divided into \textit{economic rights} and \textit{moral rights}. The economic rights authorise the rights holder to generate financial gain from allowing others to reproduce, distribute, and adapt her works. Moral rights protect the non-commercial interests of authors.\textsuperscript{130} In civil law jurisdictions, they are enforced as separate rights alongside economic rights. Moral rights are afforded to

\begin{itemize}
  \item \textsuperscript{124} Intellectual Property Office U.K. (2011), p. 14
  \item \textsuperscript{125} Directive 2006/116/EC § 1(1)
  \item \textsuperscript{126} Directive 2006/116/EC § 2(2) reads: "The term of protection of cinematographic or audiovisual works shall expire 70 years after the death of the last of the following persons to survive, whether or not these persons are designated as co-authors: the principal director, the author of the screenplay, the author of the dialogue and the composer of music specifically created for use in the cinematographic or audiovisual work."
  \item \textsuperscript{127} Directive 2006/116/EC § 3(3)
  \item \textsuperscript{128} Id. § 3(4)
  \item \textsuperscript{129} Directive 2011/77/EU § 1(2)(a)
  \item \textsuperscript{130} Bently & Sherman (2009), p. 241
\end{itemize}
authors and performing artists. \textsuperscript{131} Production, broadcasting, and publishing firms have only economic rights. \textsuperscript{132}

Moral rights are designed to protect the reputation, freedom and honour of authors. \textsuperscript{133} The scope of moral rights varies to some extent between jurisdictions, but in general countries recognise at least the \textit{right of attribution} (a.k.a. paternity right) and the \textit{right to the integrity of the work}. \textsuperscript{134} Article 6\textsuperscript{bis} of the Berne Convention states:

\begin{quote}
the author shall have the right to claim authorship of the work and to object to any distortion, mutilation or other modification of, or other derogatory action in relation to, the said work, which would be prejudicial to his honor or reputation.
\end{quote}

The \textit{right of attribution} (paternity right) affords the author a right to be made known to the public as the creator of the work, prevent others from naming another person as the author (‘right to prevent plagiarism’), and prevent others from wrongfully attributing an author to a work she has not created (‘right to prevent false attribution of authorship’). \textsuperscript{135}

The \textit{right to the integrity of the work} authorises the author to prohibit any modifications, alterations or mutilations to the work. \textsuperscript{136} The author also has an exclusive right to make changes to her work or authorise others to do so. \textsuperscript{137}

Further, some jurisdictions extend the moral rights to encompass a right to create a work, publish or not to publish a work, withdraw a published work from the market, as well as prevent libel, slander and other violations of the author’s personality. \textsuperscript{138}

Moral rights are considered to be a personal right of the author and therefore they are inalienable from her. \textsuperscript{139} Hence, an author cannot assign her moral rights to a third party. \textsuperscript{140} She can merely choose to waive her moral rights “\textit{only in regard of use

\begin{footnotes}
\item[131] Cf. Gramex (n.d. b)
\item[132] WIPO (n.d. a)
\item[133] Strauss (1959), p. 123
\item[134] WIPO (n.d. a)
\item[135] Strauss (1959), p. 116
\item[136] Id. p. 118
\item[137] Id.
\item[138] Id. p. 120-123
\item[139] Id. p. 123
\item[140] Cf. Bently & Sherman (2009), p. 258
\end{footnotes}
limited in character and extent.”¹⁴¹ For instance, she can waive her right to be identified as the creator of the work.¹⁴²

### 2.5. MONETISING COPYRIGHTS

The economic rights of copyright are commodities. They can be bought, sold, and licensed.¹⁴³ If a third party wants to exploit a copyrighted work, a contractual transfer of copyright is needed. A transfer can be made in a form of a license or an assignment. The rights are usually exchanged for money. The monetary compensation that rights holders receive from licensing works is referred to as royalties.

Copyright law recognises two types of licenses: voluntary licenses and compulsory licenses. A voluntary license constitutes permission from the licensor (the one who licenses) to the licensee (the one who is granted a license) allowing the licensee to do certain acts¹⁴⁴ such as manufacture CDs of a master tape of a sound recording, translate a book, remix a song, publish a photograph on a website, or broadcast a film on a television network. A voluntary license can be exclusive or non-exclusive. With an exclusive license the licensee can secure that nobody else is granted similar exploitation rights. Non-exclusive licenses enable the licensor to permit an unlimited number of licensees to exploit her work. A license can be further limited temporarily and geographically.¹⁴⁵ A license can be a one-off permission or for a fixed period of time. It can grant a right to sell a work in the EU but prohibit the sales in the United States.

A license is a partial transfer of copyright. When a rights holder licenses a work, the ownership of the work stays with her. She merely grants limited exploitation rights.

A compulsory license is a license imposed on rights holders on the part of the state. Compulsory licenses are rare exceptions.¹⁴⁶ The use of compulsory licenses varies between jurisdictions. A starting point in copyright law is that rights holders have a

---

¹⁴¹ Copyright Act 404/1961 (Finland) § 3(3)
¹⁴² U.K. Intellectual Property Office (n.d. b)
¹⁴³ Cf. Jacob et al. (2004), p. 5
¹⁴⁴ Bently & Sherman (2009), p. 264
¹⁴⁵ Id.
¹⁴⁶ Id. p. 270
right to decide whether they want to license their copyrights. A compulsory license limits this right. A compulsory license forces the rights holder to license her work and requires the licensee to pay a fee as remuneration to the rights holder. In Finland, compulsory licenses cover some specific uses of compilations in teaching and making works available to the visually and hearing impaired.

The author can also assign her copyrights. “An assignment is a transfer of ownership of the copyright.” In an assignment, the author can transfer all her rights (reproduction, adaptation, and distribution) to all territories indefinitely. Alternatively, she can choose to assign only certain rights with territorial restrictions for a specified time period. An assignment presumes exclusivity and usually limits the author’s right to use her own work parallel to the new owner of the rights.

### 2.5.1. The Role of Collective Management Organisations

Rights holders who make a living from the licensing of their works often appoint a collective management organisation (CMO) to “administer the licensing of rights, collection of royalties, and enforcement of rights on their behalf.” CMOs grant licenses to firms and individuals who use copyrighted works. They collect licensing fees from users and re-distribute them as royalties to rights holders.

CMOs can grant two types of licenses to content users: individual licenses concerning the exploitation of one specified work and blanket licenses for mass uses of content. In practice, blanket licenses most often concern the use of music on television, radio, and the Internet. A blanket license is a license, which for an annual fee allows a broadcaster to perform any song from a music repertory that the CMO administers. Without a blanket license, a broadcaster would have to ask permission separately from each composer, lyricist, performing artist, and record publisher. This would make the broadcasting of music infeasible.

---

147 Bently & Sherman (2009), p. 270; Nettilaki (2013)
148 Bently & Sherman (2009), p. 270
149 Nettilaki (2013)
150 Bently & Sherman (2009), p. 262
151 Cf. id.
152 IPOS (2013)
153 Cf. ASCAP (2013)
A special kind of a blanket license exists in the Nordic countries and the EU in a form of extended collective licensing (ECL). In the context of ECL, copyright law grants CMOs a mandate to administer also the licensing of rights on behalf of authors who are not their clients. The difference between a traditional blanket license and an extended collective license is that extended collective licenses also cover works from rights holders that the CMO does not represent.

In order for the blanket licensing and ECL regimes to function efficiently CMOs must collaborate. For instance, when a Finnish radio channel plays a song of a German singer-songwriter, two Finnish CMOs, Teosto and Gramex, collect licensing fees from the radio channel and distribute them to their partner CMOs, GEMA and GVL in Germany, which distribute the royalties to the German artist in question. It is also possible that the German artist was a client of the Finnish CMO, in which case, the Finnish CMO would distribute the royalties directly to her. If the German artist was not a client of any CMO, copyright laws in countries that apply ECL allow her nonetheless to claim remuneration from the use of her works. According to Finnish copyright law, such claims must be made within three years from the end of the calendar year during which the reproduction, communication or transmission of the work took place.

2.5.2. Creative Commons Licenses

It was mentioned earlier in this chapter that copyright comes into being automatically. From this follows that the author cannot decide whether her work is copyrighted. However, an author, who does not have an agreement with a CMO, can make a decision not to enforce her rights. An author, who has appointed a CMO to administer her rights, usually cannot turn a blind eye on third-party uses of her works unless her agreement with the CMO allows her to decide in which circumstances third parties need licenses.

---

154 Cf. Vuopala (2013); European Broadcasting Union (n.d.)
155 Teosto represents composers, lyricists, arrangers, and music publishers (Teosto, 2012).
156 Gramex represents producers of sound recordings and performing artists, whose performances have been recorded on sound recordings (Gramex, n.d. a).
157 GEMA represents composers, lyricists, and music publishers (GEMA, 2010)
158 GVL represents performing artists and record manufacturers (GVL, 2004)
159 Copyright Act 404/1961 (Finland) § 26(5)
An author can also decide not to monetise her works but ask that third parties merely respect her moral rights. In such cases the author can license her works under Creative Commons (CC) licenses. CC licences are not codified in copyright laws. They offer an alternate licensing scheme for voluntary copyright licenses. Should someone breach a CC licensing agreement the licensor can sue on the grounds of breach of contract but not on the grounds of copyright infringement.

There are six different types of CC licenses. All six licenses are worldwide, royalty-free, non-exclusive, perpetual, “copyleft” licenses. This means that works are reproduced and distributed without geographical limitations and paying licensing fees. The license is in force indefinitely and an unlimited number of re-users can exploit the work. It is noteworthy that an author cannot waive a compulsory copyright license. This means that should a state impose a compulsory license on a work, the author is required to collect copyright fee from the users of her CC-licensed work.

All CC licenses require that the name of the author be mentioned when the work or derivative works made of it are shared. Hence, the benefits of CC licenses are reputational. The author may also require that her work is not used for commercial purposes or altered in any way, or that the re-user publishes her work using an identical license with the original license.

2.6. LIMITATIONS TO COPYRIGHT

If you want to copy, distribute, or adapt a copyrighted work, you generally need a license from the rights holder. However, there are a few situations in which you do not need an authorisation to use a work. These special situations are in copyright referred to as the limitations and exceptions to copyright. They limit rights holders’ rights to control the use of their works.

Article 9(2) of the Berne Convention stipulates that countries can at their own discretion enact limitations to copyright laws, which permit the use of works or parts of

---

160 Creative Commons (n.d. b)
161 See: Id. (n.d. c)
162 Id.
163 Creative Commons (n.d. b)
164 Id.
them without authors’ permission. Such limitations must fulfil three criteria. A reproduction without authorisation can be permitted if it occurs (1) in certain special cases, provided that such reproduction (2) does not conflict with the normal exploitation of the work, and (3) does not unreasonably prejudice the legitimate interests of the author. These principles form the so-called Berne Three-Step Test. Legislators use the test in designing new copyright limitations and evaluating the fairness of existing limitations when revisions are called upon as a consequence of technological advancements. Also, tribunals often refer to the Three-Step Test when evaluating the legitimacy of new technologies and service models.

Copyright limitations vary between jurisdictions. Some copyright laws introduce exhaustive lists of copyright limitations while some rely more on general rules such as fair dealing and fair use. Nevertheless, a few universal principles can be identified.

For instance, individuals and commercial actors have a right to make quotations from protected works.165 There are however four prerequisites for making legitimate quotations. Firstly, the work being quoted must have been made lawfully available to the public.166 In other words, the work being quoted has to be a published work and the rights holder must have authorised its publication. Also, the name of the author and the source of the work (e.g. the name of the newspaper) have to be mentioned.167 Further, the extent of a quotation may not exceed what can be considered as fair practice or proper usage.168 This means that the amount of how much one can freely copy from a protected work depends on the purpose of the quotation. For example, if a business student copies an extensive portion or a substantial part of a scientific article into her master’s thesis, she is likely to exceed the quotation right. However, a literature student who in her thesis analyses the writing style of a novelist is allowed to copy extensive and substantial parts into her study, as she must be able to demonstrate how she has reached her conclusions.

Additionally, countries may permit copyright limitations, which allow the press to reproduce and communicate works or parts of works without authorisation in reporting current events as news stories and critical reviews.169 However, this right is usually limited. A general rule is that the original source of the work must be

---

165 Berne Convention § 10(1)
166 Cf. id.
167 Id. § 10(3)
168 Id. § 10(1)
169 Cf. id. § 10bis
indicated in connection to the reproduction.\textsuperscript{170} Also, a law may allow an author to expressly prohibit the re-use of her works in news reporting.\textsuperscript{171}

Generally, private citizens are also allowed to reproduce works exclusively for their personal, private, and non-commercial use.\textsuperscript{172} A prerequisite is that the work has been lawfully made available to the public. This means that the work being copied has to be a published work, the publication of which has been authorised by the rights holder. Many countries limit the \textbf{private reproduction right} on digital platforms.\textsuperscript{173} The right to copy digital works is usually limited to the reproduction of single copies.\textsuperscript{174} The reproduction of some works may not be permitted at all. For instance, a reproduction of a computer programme for a private use is not permitted in Finland\textsuperscript{175} except for making a backup copy, if it is necessary for the use of the programme for the intended purpose.\textsuperscript{176} Also, technological protection measures (TPMs), which many publishers use to protect their digital books, films and music, limit private copying. The circumvention of TPMs is prohibited by virtue of international copyright treaties\textsuperscript{177} and national laws.

Countries that allow private copying are obligated to provide a fair financial compensation to rights holders for the reproduction of their works.\textsuperscript{178} The compensation is carried out in a form of private copying levies. A levy is a payment paid by a manufacturer or an importer of a device that can be used to reproduce works.\textsuperscript{179} For instance, a levy is paid from computers, external hard drives, memory sticks, mobile phones, recordable CDs and DVDs and other recordable blank media.

Yet another important limitation is \textbf{copyright exhaustion} (a.k.a. first-sale doctrine), which limits the author’s right to control the distribution of her works or copies made of them. Copyright exhaustion means that when a rights holder or an authorised third party offers a work or copies of it to the market by the means of sales or other transfer of ownership, the rights holder can no longer exercise her rights in relation to the sold

\textsuperscript{170} Berne Convention § 10\textsuperscript{bis}(1)
\textsuperscript{171} Id.
\textsuperscript{172} WIPO (n.d. a)
\textsuperscript{173} Id.
\textsuperscript{174} Cf. Copyright Act 404/1961 § 12(1)
\textsuperscript{175} Id. § 12(4)
\textsuperscript{176} Id. § 25j(1)(2)
\textsuperscript{177} Cf. WCT § 11, 12; WPPT § 18
\textsuperscript{178} Cf. Directive 2001/29/EC § 5(2)(b)
\textsuperscript{179} Cf. Copyright Act 404/1961 § 26a(1)
work or copies.\textsuperscript{180} This means that when a publishing company authorises a bookshop to sell their copies of books, the publisher can no longer control what happens to a copy when an individual buys it. The buyer has a right to re-sell and lend her copy of the book to a third party. However, she is not allowed to make copies of the book and start selling or lending those copies. Unfortunately, uncertainty exists in terms of whether copyright exhaustion applies to digital copies of works.\textsuperscript{181} Under the current interpretation of copyright laws, the EU applies copyright exhaustion to computer programmes\textsuperscript{182} but not to other digital literary, artistic, and musical works.\textsuperscript{183} In the United States, copyright exhaustion does not apply to the resale of digital music files.\textsuperscript{184}

Furthermore, many countries provide some additional reproduction and communication rights without authorisation for non-profit organisations such as schools, universities, research institutions, libraries, museums and archives.\textsuperscript{185} Also, the reproduction and distribution of works adapted into a form of a parody or satire are commonly acknowledged limitations to copyright.\textsuperscript{186}

\subsection*{2.6.1. Fair Use In the United States}

Apart from specific statutory limitations to copyright, common law countries additionally apply a principle of fair dealing or fair use in defining whether an act of reproduction, distribution, or adaptation can be held legal. The United States is an example of a country that has codified the principle of fair use to its copyright legislation. American courts commonly use the fair use doctrine as a basis in analysing alleged infringing uses of copyrighted works.

Title 17 USC § 107 stipulates that in determining whether a use of a work can be interpreted as fair use, four factors are to be considered:

1. The \textit{purpose and character of the use}, including if such use is of a commercial nature or is for non-profit educational purposes;

\textsuperscript{180} WIPO (n.d. c)  
\textsuperscript{181} Cf. Phillips (2013)  
\textsuperscript{182} Cf. UsedSoft GmbH v. Oracle International Corp., CJEU Case C-128/11, April 24, 2012  
\textsuperscript{183} Cf. Phillips (2013)  
\textsuperscript{184} Cf. Capitol Records, LLC v. ReDigi, Inc., No. 12 Civ. 95 (RJS), March 30, 2013  
\textsuperscript{185} Cf. Directive 2001/29/EC § 5(2)(c)  
\textsuperscript{186} Cf. Bimbaite (2004)
2. The **nature of the copyrighted work**;

3. The **amount and substantiability of the portion used** in relation to the copyrighted work as a whole; and

4. The **effect** of the use **upon the potential market for or value of the copyrighted work**.

The first principle relates to for what purpose an unauthorised re-user (person or firm) uses the copyrighted work. If a work is re-used for commercial purposes to achieve financial gain it is more likely that a court deems the use unfair. It is noteworthy that a direct economic benefit is not required to demonstrate a commercial use.\(^{187}\) Case law suggests that a repeated and exploitative copying of copyrighted works, even if the copies were not offered for sale, can constitute a commercial use.\(^{188}\)

In defining the nature of the copyrighted work, a court evaluates whether the copyrighted work that has been re-used is a published or an unpublished work and whether the work is factual or creative.\(^{189}\) An unauthorised use of an unpublished or a creative (“fictive”) work is more likely to be defined unfair and hence infringing.\(^{190}\)

In determining the amount and substantiality of the portion used, a court evaluates how much the re-user has used of the copyrighted work in quantitative terms and whether that what has been copied forms qualitatively a substantial part of the work.\(^{191}\) The more the unauthorised re-user has used from the work and the more she has utilised substantial parts of the work, the more likely it is that she infringes copyright.

In analysing the market effect of an unauthorised use of a work a court determines how the work of the re-user influences the market or the value of the original work.\(^{192}\) If the work of the re-user substitutes the original work in the market, the more likely it is that the use is deemed unfair. However, even if a re-use caused harm to the sales of the original work a court can in certain circumstances regard the re-use as non-

---

\(^{187}\) Cf. A&M Records Inc. v. Napster Inc. 239 F.3d 1004 at 26

\(^{188}\) Id.

\(^{189}\) University of Minnesota (2010)

\(^{190}\) Id.

\(^{191}\) Id.

\(^{192}\) Id.
infringing.\textsuperscript{193} For instance, this could happen if a court were to interpret a re-use as ‘transformative’.

Since the mid 1990’s American courts have applied a fifth factor in determining whether an unauthorised use can be considered fair use.\textsuperscript{194} This factor is \textit{transformative use}.\textsuperscript{195} The principle derives from a Supreme Court ruling from 1994.\textsuperscript{196} Within this rule a derivative work can be fair use if the re-user has used the source work in completely new and unexpected ways.\textsuperscript{197}

\section*{2.7. COPYRIGHT LIABILITY, SANCTIONS AND REMEDIES}

A copyright infringement occurs when in the absence of copyright limitations a person reproduces, distributes, or adapts a copyrighted work without permission from the rights holder or violates a rights holder’s moral rights.

An alleged infringer can be found guilty on the basis of a direct (primary) infringement or an indirect (secondary) infringement.\textsuperscript{198} Direct liability emerges when a person uses a work herself without asking permission from the rights holder.\textsuperscript{199} An indirect infringement may take place when a person induces, facilitates, assists, or otherwise encourages another person to infringe copyrights.\textsuperscript{200} A mere knowledge of an infringing potential of a technology that one sells or offering customers technical support with regard to how to use a technology that can be used for violating copyrights does not necessarily lead to indirect liability.\textsuperscript{201} Indirect liability presupposes “\textit{purposeful, culpable expression and conduct}”.\textsuperscript{202} Also, failing to take reasonable and effective measures to curtail infringement can lead to the emergence of indirect liability.\textsuperscript{203} A prerequisite for an indirect infringement is an existence of a direct infringement. This

\begin{thebibliography}{99}
\bibitem{193} Id.
\bibitem{194} University of Minnesota (2010)
\bibitem{195} Id.
\bibitem{197} Cf. id.
\bibitem{198} Cf. Stern (2004)
\bibitem{199} Cf. id.
\bibitem{200} Cf. id.
\bibitem{201} Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd, 545 U.S. 913 (2005), p. 19
\bibitem{202} Id.
\bibitem{203} Allen (2008), p. 87
\end{thebibliography}
means that a rights holder has to be able to establish a direct infringement before she can accuse someone of an indirect infringement.

The copyright doctrine of indirect liability has emerged largely as a result of case law. Courts began to impose indirect liability as a consequence of not being able to enforce copyright laws against direct infringers, who often were end-users.\textsuperscript{204} In defining indirect copyright liability courts have sought support from common law tort laws\textsuperscript{205} and patent laws.\textsuperscript{206} In the United States, case law has created the copyright doctrines of contributory and vicarious liability.\textsuperscript{207} The doctrine of authorisation liability dominates the legal practice in the United Kingdom and Australia.\textsuperscript{208} Indirect liability in German courts translates into Störerhaftung.\textsuperscript{209} In the Nordic countries, where the concept of indirect liability does not exist as such, a person can be found liable for being a contributor,\textsuperscript{210} co-infringer\textsuperscript{211} or on the basis of assisting in copyright violations.\textsuperscript{212}

The enforcement of copyright laws usually takes place in civil courts.\textsuperscript{213} Sanctions in civil cases include payments of monetary damages.\textsuperscript{214} Deliberate infringements on a commercial scale, such as counterfeits of physical goods\textsuperscript{215} or a wide-scale unauthorised distribution of copyrighted works on the Internet,\textsuperscript{216} can result in criminal charges. Criminal courts are authorised to sanction offenders with fines and imprisonment.\textsuperscript{217} In addition, both civil and criminal courts have the power to order a party to prevent the entry into channels of commerce where infringements take place.\textsuperscript{218} Courts can also require the recall and permanent removal of infringing goods from the channels of commerce and the destruction of infringing goods and materials used in manufacturing.

\textsuperscript{204} Allen (2008), p. 88
\textsuperscript{205} Cf. Jha & Jha (2006)
\textsuperscript{206} Cf. Stern (2004)
\textsuperscript{207} Cf. id.
\textsuperscript{208} Cf. Napthali (2005), Seng (2008)
\textsuperscript{209} Cf. GEMA v. YouTube Az. 310 O461/10, April 20, 2012
\textsuperscript{211} Cf. Finreactor, KKO:2010:47
\textsuperscript{212} Cf. Activision Publishing Inc. et al. v. Fredrik Neij et al., Mål nr B4041-09, Svea Hovrätt (2010)
\textsuperscript{213} Cf. Jacob et al. (2004), p. 5
\textsuperscript{214} Cf. id.
\textsuperscript{215} Cf. id.
\textsuperscript{216} For instance, in 2012 the United States Department of Justice charged the leaders of the file sharing service Megaupload with a criminal copyright infringement on the basis of massive worldwide online distribution of unauthorised content. More information: The United States Department of Justice (2012): “Justice Department Charges Leaders of Megaupload with Widespread Online Copyright Infringement.”
\textsuperscript{217} Jacob et al. (2004), p. 5
\textsuperscript{218} See: TRIPS § 44
Because it can take years before a legal dispute is solved, courts can also order so-called interlocutory (preliminary) injunctions. An interlocutory injunction orders an alleged infringer to stop doing the acts that result in infringements. In the context of online media services, receiving an interlocutory injunction usually means that the service provider must shut down its servers or at least those parts of the service where infringements take place. This often halts the service provider’s business.

2.8. LIABILITY LIMITATIONS OF INTERNET SERVICE PROVIDERS

A typical online media service provider facilitates user interaction, hosts a file storing service, aggregates information, or provides an access to the Internet. In common parlance such firms are often referred to as Internet service providers (ISPs). Copyright law acknowledges such firms as intermediary service providers.

Indeed, ISPs are often intermediaries. They operate between traditional publishing companies and end-users. They typically re-use copyrighted works or allow their service users to re-use copyrighted works. As a consequence ISPs are in great danger of infringing copyrights either directly or indirectly.

In certain occasions, ISPs are able to escape copyright liability on the basis of the so-called ISP safe harbours (a.k.a. ISP liability limitations). The national treatment of ISP safe harbours varies. In the United States, ISP liability limitations are coded in Section 512 of the United States Copyright Act referred to as the Title 17 USC (United States Code). In the EU, they are coded in Directive 2000/31/EC, which is here referred to as the E-Commerce Directive. The intent of the safe harbour provisions is to protect innovation by providing liability limitations for companies that serve as conduits for user interaction and user-generated content.

In the E-Commerce Directive, the ISP liability limitations are stated in Articles 12-15. Article 12 exempts an ISP acting as a mere conduit from copyright liability if it:

(a) Does not initiate the transmission;

---

219 Enforcement Directive 2004/48/EC § 10(1)
221 Seng (2008), p. 5
222 Smith (2011), p. 1580
(b) Does not select the receiver of the transmission; and
(c) Does not select or modify the information contained in the transmission.

Further, an ISP can qualify for the ‘mere conduit exemption’ if the act of transmitting information is a part of a technological process, the sole purpose of which is to enable a transmission of information in a communications network. In addition, Article 12(2) requires that a “mere conduit” does not store information on its servers “for any period longer than is reasonably necessary for the transmission”. Article 12(3) further obligates a “mere conduit” to terminate or prevent an infringement if it receives an order from a court.

Article 13 of the E-Commerce Directive exempts ISPs from copyright liability when they are involved in caching information as a part of an automatic, intermediate and temporary storing process of information, where the storing is performed for the sole purpose of making the transmission more efficient. The additional criteria to be fulfilled are:

(a) The provider does not modify the information;
(b) The provider complies with conditions on access to the information;
(c) The provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
(d) The provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
(e) The provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at 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.

Additionally, ISPs are obligated to terminate or prevent an infringement from occurring if a national court so orders.

According to Article 14, ISPs that provide hosting services can be exempt from copyright liability if in the context of providing a storing service:

(a) The provider does not have actual knowledge or information of illegal activity and is not aware of the facts or circumstances from which the illegal activity or information is apparent; or
(b) The provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

A hosting service provider is also required to terminate or prevent an infringement should a national court impose an order.

Indeed, Article 14(1)(b) requires that when an ISP receives information about an infringement, it is required to remove the infringing content or to disable the access to the infringing content without delay. An ISP usually receives the information about an alleged infringement from a rights holder in a form of a complaint letter. In the United States, these complaints are often referred to as DMCA takedown notices. In Europe they are known as takedown notices or cease-and-desist requests. The notice-and-takedown procedure in the United States is well defined in Title 17 USC §512(c). In the EU, there currently are no formal requirements for how the procedure should be carried out. A draft of a directive is working its way through the European Commission at the time of writing this thesis.223

Article 15 of the E-Commerce Directive stipulates that national authorities cannot impose general monitoring obligations on ISPs. This means that an ISP cannot be obligated to actively seek facts or circumstances that would reveal illegal activities. The preamble of the E-Commerce Directive demarcates the rule “No General Obligation to Monitor” by stating that the exemption from a monitoring obligation concerns only obligations of a general nature but not monitoring obligations in a specific case.224 Further, public authorities can require an ISP to disclose information about its service users who are suspected of illegal activities.

---

223 Horten (2013)
224 Directive 200/31/EC, Preamble at 47
3 LEGALITY OF ONLINE MEDIA SERVICES

Technological innovation has the capacity to shape business models. Respectively, business models can be viewed as a source of innovation in themselves. The concept of 'business model' became prevalent only in the mid of 1990’s alongside with the development of the Internet. This may indicate that on the Internet the technology and the business model are closely intertwined.

When a court is asked to decide on the legitimacy of an e-service, one of the first things it does is to examine the technologies that have been used to carry out the service. This examination leads the court to study software and hardware functionality.

In this chapter, we explore how copyright relates to the functioning principles of the Internet. We also examine how the technology can contribute to the emergence of copyright liability. The chapter will not constitute a software engineering handbook or an in-depth legal analysis. Rather, the objective is to help people who do not have a technical or legal background to understand what kinds of legal risks are involved in operating a business on the Internet.

3.1. ARE LINKING AND FRAMING ALLOWED?

3.1.1. Hyperlinking

“Nils Svensson, a journalist, wrote an article for a Swedish newspaper that was published in print and on the newspaper’s website. Retriever Sverige AB, the defendant in the case, offers a subscription-based service, whereby customers can access newspaper articles; the articles are however not available on the Retriever’s website but merely linked to the original, third-party source. Svensson sued Retriever for “equitable remuneration”, arguing that Retriever had made his article available through the search and alert functions on its website. This, he maintains, falls within the copyright relevant acts of either communication to the public or the public performance of a work, for either of which he has not given consent.”

---

225 Zott et al. (2010), p. 19
226 Id.
227 Id. p. 4
228 De Beer & Burri (2013), p. 17-18
Nils Svensson v. Retriever Sverige AB\textsuperscript{229} is a pending EU case referred by Svea Appeals Court of Sweden (Svea Hovrätt) to the Court of Justice of the European Union (CJEU). Svea Appeals Court asks CJEU to help it to interpret EU copyright legislation. It asks: “If anyone other than the holder of copyright in a certain work supplies a clickable link to the work on his website, does that constitute communication to the public within the meaning of Article 3(1) of Directive 2001/29/EC […]?”

There is no doubt that the Internet and digital technologies have destabilized the global copyright system.\textsuperscript{230} Recently, there “has been much discussion about whether a website operator infringes copyright in a work by providing a link to another website containing that work, or framing through to that work.”\textsuperscript{231} In lawsuits, in which the legality of linking or framing is questioned, courts unavoidably come close to ruling on the legitimacy of basic Internet functionality. Consequently, in deciding on the Svensson case CJEU will face a great pressure, as the ruling will have far-reaching implications. The decision is expected in 2014.

“A hyperlink is a word, phrase, or image that you can click on to jump to a new document or a new section within the current document.”\textsuperscript{232} The Internet would not function without hyperlinks (‘links’). Links constitute paths leading users from one location to another.\textsuperscript{233} Without links we could not locate or access information. Hence, it can be argued that linking is the single most important feature of the Internet.\textsuperscript{234}

However, technically linking could be considered to be a copyright infringement if the link directs us to works that we do not have permission to use.\textsuperscript{235} It has been argued that creating a link constitutes making available\textsuperscript{236} or communicating\textsuperscript{237} works to the public, or reproducing works.\textsuperscript{238} If any of the claims were true, any person who posted a link would need permission from the owner of the work to which the link referenced. Without a reasonable compulsory licensing regime or an expansion of copyright

\begin{footnotesize}
\begin{enumerate}
\item Nils Svensson, Sten Sjögren, Madelaine Sahlman, Pia Gadd v Retriever Sverige AB, CJEU, Case C-466/12, OJ 2012 C 379/31 [Svensson]
\item De Beer & Burri (2013), p. 3
\item Silverman (2012)
\item TechTerms.com (2013)
\item Bently et al. (2013), p. 1
\item Id.
\item Saikia (2010), p. 2
\item Id.
\item Cf. Bently et al. (2013), p. 11
\item Silverman (2012)
\end{enumerate}
\end{footnotesize}
exceptions the publishing of information would practically become infeasible and the Internet would come to a standstill.

In early 2013, European Copyright Society, a group consisting of prominent European legal scholars,\textsuperscript{239} issued an opinion in reference to the Svensson case. Their aim is to influence CJEU in decision-making. They ask CJEU to rule that hyperlinking does not constitute an activity covered by the right to communicate works to the public.\textsuperscript{240}

There are several court decisions that support the view of the European Copyright Society. In the Norwegian napster.no case,\textsuperscript{241} a consortium of copyright organisations and record labels asked the Court to rule that hyperlinking would constitute an act of making works available to the public or alternatively that linking to unauthorised MP3 files would constitute contributory infringement.\textsuperscript{242} The Court refused to recognise hyperlinking as an act of making available to the public and found napster.no liable for contributory infringement on the grounds of participating in infringements (“medvirkningsansvar”).\textsuperscript{243} The court reasoned:

“[I]f hyperlinking is to be regarded as making available to the public […], then this must be so regardless of whether the material being linked to is of a legal or illegal nature. Further, the judgment as to whether hyperlinking is covered by the exclusive rights of the copyright holder or not cannot [… ] be affected by which type of link is being used […].”\textsuperscript{244}

With this statement, the Supreme Court of Norway addressed a fundamental problem. If it had ruled that hyperlinking in the napster.no case constituted copyright infringement, the consequences would had been much more pervasive. Hyperlinking as such, even in cases of directing traffic to legitimate content, would have become an exclusive right of rights holders. By the same token the Court stated that posting an URL (Uniform Resource Locator web address), without generating a hyperlink, with the intent to inform Internet users about a location of a work could not be regarded as making works available to the public.\textsuperscript{245}

\textsuperscript{239} Hugenholtz (2013)
\textsuperscript{240} Bently et al. (2013), p. 2
\textsuperscript{241} TONO mfl, EMI Norsk AS mfl mot A. 27.01.2005, HR-2005-00133-A (sak nr. 2004/822)
\textsuperscript{242} Rieber-Mohn (2005)
\textsuperscript{243} Id.
\textsuperscript{244} Id.
\textsuperscript{245} Id.
Hyperlinking can be carried out in many different ways. One way is to use so-called 'deep links'. "Deep linking allows visitors to bypass information and advertisements at the home page and go directly to an internal page"\(^\text{246}\) on a website. Many website owners dislike deep linking, because they can lose income if their revenues are dependent on the amount of visitors that enter the website through the home page where advertisements are located.\(^\text{247}\)

In 2005, the Supreme Court of Germany (Bundesgerichtshof) decided in *Holtzbrinck v. Paperboy*\(^\text{248}\) that the Internet search engine *Paperboy* did not violate the rights of *Holtzbrinck* publishing house by providing on the Internet and via email a list of search results that included snippets of *Holtzbrinck’s* newspaper articles and deep links to *Holtzbrinck’s* newspaper websites.\(^\text{249}\) The Court found that neither the use of short fragments of the newspaper articles nor the deep links amounted to an infringement.\(^\text{250}\) The Court stated that each fragment in itself was too insubstantial to constitute a literary work and thus they were not relevant copies under the provisions of copyright.\(^\text{251}\) According to the Court the primary function of the deep links did not go beyond that of a footnote or other reference in a printed document.\(^\text{252}\)

The insubstantiality of the fragments was a determining factor in why the Court also found that *Paperboy’s* use of links could not conflict with the normal exploitation of *Holtzbrinck’s* database rights.\(^\text{253}\) The Court added that the fragments “did not constitute a substantial part of the database” and that “the utilization of the short fragments did not replace but rather stimulated the further use of the databases”.\(^\text{254}\)

It is noteworthy that the Supreme Court did not confirm whether *Holtzbrinck’s* collection of newspaper articles could be protected as a database. The Court merely noted that if the article collection were to be considered as a database, *Paperboy* would not infringe *Holtzbrinck’s* rights. Hence, the *Paperboy* ruling does not shed light on whether a collection of articles, a list of links, or an index could constitute copyrightable subject matter under database provisions.

\(^{246}\) Fitzpatrick (2013)

\(^{247}\) Id.

\(^{248}\) Holtzbrinck v. Paperboy I ZR 259/00 (17 July 2003) [2005] ECDR (7) 67, 77

\(^{249}\) Cf. Stemplewitz (2006), p. 373-375

\(^{250}\) Id. p. 373

\(^{251}\) Id.

\(^{252}\) Id.

\(^{253}\) Id.

\(^{254}\) Id. p. 374
The Court also ruled that Paperboy could not be held liable for contributory infringement, as Paperboy merely provided an access to articles, which Holtzbrinck already had made available to the public without any technical protection measures.\textsuperscript{255} The Court noted that Holtzbrinck could implement technical protection measures at any time if it wanted to prevent search engines to access its content.\textsuperscript{256} In addition, Holtzbrinck could also make a decision to remove the articles from the Internet should they not want to continue to make the articles available to the public.\textsuperscript{257}

The Court further rejected Holtzbrinck’s argument that its legitimate interests were violated as a consequence of Paperboy’s choice to use deep links, which bypassed advertisements on Holtzbrinck’s home page. The Court opined that Holtzbrinck could neither demand nor expect that a freely available document on the Internet could be accessed only one way, which in this case was a more cumbersome method than accessing the article directly through the deep link. The Court reasoned that with deep links Paperboy “provided an effective method of retrieving and filtering the tremendous amount of information available on the [I]nternet”.\textsuperscript{258}

One of the first court decisions concerning the legitimacy of deep linking dates back to 2002 in Denmark, where the District Court (Københavns Byret) came to quite an opposite conclusion. In the lawsuit, Danske Dagblades Forening (hereafter DDF), an association representing Danish newspapers, asked the Court to prohibit the website operator Newsbooster from providing deep links to newspaper articles on its website and as electronic newsletters via email.\textsuperscript{259} Newsbooster argued that it was a search engine and hence exempt from liability under ISP safe harbour provisions.\textsuperscript{260} The Court refused Newsbooster’s claim; Newsbooster could not be held as a search engine, because the creation of the infringing newsletters required an active participation on the part of Newsbooster.\textsuperscript{261} Instead, the Court opined that Newsbooster’s service was in direct competition with the newspapers. It did not produce the content of its newsletters but rather it used the newspapers’ content. It also generated income with this activity. Further, the newspapers in question lost advertising income, because deep

\textsuperscript{255} Stemplewitz (2006), p. 373
\textsuperscript{256} Id.
\textsuperscript{257} Id.
\textsuperscript{258} Id. p. 374
\textsuperscript{259} Cf. Danske Dagblades Forening v. Newsbooster Aps, sag nr. FS F1-8703/2002
\textsuperscript{260} Id.
\textsuperscript{261} Id.
links allowed users to bypass the home pages of the newspapers. Consequently, the Court found that the actions of Newsbooster were against good marketing practice.

In addition, the Court sided with DDF in its claim that the newspapers’ collections of article texts and article headlines enjoyed catalogue protection. As a consequence, the Court found that Newsbooster violated the newspapers’ database rights.

In Paperboy and Newsbooster the plaintiffs claimed that headlines and short excerpts of newspaper articles constituted copyrightable subject matter. In Paperboy, the Court concluded that the snippets that Paperboy used were too insignificant to form an independent copyrightable work. In Newsbooster, the Court ruled that database rights could protect collections of headlines and article texts, if a significant amount of work was involved in creating the collections. This means that posting headlines of newspaper articles embedded in hyperlinks or URLs or displaying a sentence or two of the original article as part of search results could result in copyright infringement.

The legitimacy of using headlines in links was tested already in 1996 in an Irish case Shetland Times Ltd. v. Wills, et al. The Shetland Times newspaper sued its rival The Shetland News for copyright infringement and unfair competition. It accused The Shetland News of copying the headlines of its articles to form links, which were distributed on the website of The Shetland News. The Shetland Times argued that readers could mistake its works for the works of The Shetland News. The case was settled after the Court’s interlocutory decision, which suggested that headlines could be copyrightable. The Shetland News was granted permission to link to the headlines on two grounds: It had to include the text “A Shetland Times Story” and a button linking back to the website of The Shetland Times on its website.

---

263 Id.
264 In the Nordic countries, database protection exists also for unoriginal databases such as catalogues, tables, and other similar productions, the creation of which requires substantial resources such as time and money. More information: Olsson (1999): “Intellectual Property Rights for Non-Original Databases – The European Community Directive and the Scandinavian Experience”.
266 EFF (2011)
267 Id.
268 Id.
269 Id.
270 Id.
In 2006, the Belgian Association of Newspaper Editors Copiepresse sued Google in Belgium for infringing the copyright of newspapers with its news aggregating service Google News and some additional websites.271 Copiepresse claimed that Google infringed copyrights on two grounds: (1) linking to content on newspaper websites and (2) linking to copies of sections of stories that Google stored on its servers as part of its Google News service,272 the process of which Google referred to as caching. The Court’s decision would hence shed light not only on the legitimacy of linking but also whether Google’s implementation of the caching technology would allow it to enjoy ISP safe harbour protection. Google lost the case on both accounts first in the Court of First Instance in 2007 and again in the Court of Appeals in 2011.273 As a result, the parties entered into a settlement agreement whereby further legal proceedings were ended without an appeal to the Supreme Court.274

In the centre of the dispute was the technological solution that Google used in aggregating content in the Google News service. When a service user (referred to as ‘cybernaut’ by the Court) clicked on a cached link, Google News compiled the page for her from two sources: The text came from an archived copy of the article that Google’s web crawler (search robot) had stored on Google’s server hours or days earlier, while the graphic elements of the article were retrieved from the server of the newspaper as they appeared at the time when the user clicked the link.275 The Court noted that as a result it was not unusual that the text on the user’s computer screen was a few days older than the rest of the information, because the former emanated from Google’s “cache” memory, while the latter came from the publisher’s server.276

The technological solution of Google News resulted in three potential complications. Firstly, Google did not direct user traffic to the websites of the newspapers, from which it copied the texts and the graphics. Rather, users read the compiled articles on Google’s servers. Additionally, in certain cases, it could happen that the original author had changed the text of the article after the article was stored on Google’s server, in which case Google News displayed an old version of the article. Thirdly, Google’s “cache” storage facilitated searches even in circumstances where the original page of

271 Google Inc. v. Copiepresse R.no. 2011/2999, No. 817
272 Id.
273 Id.
274 Van Besien (2013)
275 Cf. Google Inc. v. Copiepresse R.no. 2011/2999, No. 817 at 2, 26
276 Id. at 2
the newspaper would be inaccessible. Understandably, the rights holders did not regard the actions of Google favourably.

In terms of whether Google’s linking constituted unlawful reproduction or communication to the public, the Court of Appeals stated the following:

“It has been established that Google registers on its servers a copy of the pages [...] It has also been established that when cybernauts click the “cached” link, Google transmits this copy to them. [...] only the author is entitled to copy his work or to authorise its reproduction [...] Likewise only the author is entitled to communicate it to the public [...] From this provision it can be deduced that Google’s registration [...] constitutes a physical act of reproduction. [...] the fact that Google allows cybernauts to take cognizance of this copy – which is not to be confused with the original – by clicking on the “cached” link amounts to public communication. In the digital field, the issue of reproduction arises from the moment there is a question of fixation, which makes that downloading comes under reproduction right [...].”

The fact that Google made copies of the original article texts and stored them on its servers for long periods of times without the permission of rights holders resulted in Google becoming liable for unauthorised reproduction of works. The long storage times also made it futile for Google to base its defence on the ISP caching safe harbour, because its caching function did not constitute temporary, transient or incidental reproduction but rather the cached pages were always available on the Internet by the means of normal search. Further, when Google allowed service users to access the copied texts on its servers, it became liable for unauthorised communication of works.

Even if Google had carried out its service by merely linking users directly to newspapers’ own websites, Google would not have been able to escape liability. This is because the Court of Appeals found that the excerpts that Google used in links and indices of search results constituted substantial parts of the original articles. The Court based its finding on the fact that the excerpts included the essential information that the publisher and the journalist wanted to convey to the readers. This finding alone resulted in Google becoming liable for unauthorised reproduction and communication.

277 Google Inc. v. Copiepresse R.no. 2011/2999, No. 817 at 25
278 Id. at 21, 22
279 Id. at 23, 25, 26
280 Id. at 29, 30
281 Id. at 28
The Court also denied Google’s claim that it had a right to use excerpts on the basis of the quotation right. The Court considered that the aim of Google News was to certain extent to replace the services of newspaper publishers, which made it ineligible for the quotation exemption.\textsuperscript{282} The Court further rejected Google’s argument that it qualified for the exemption of ‘press review’,\textsuperscript{283} because Google merely reproduced press articles without critiquing or commenting them.\textsuperscript{284} Nor was Google eligible for the ‘news bulletin’, exception. The Court opined that cached articles do not constitute news bulletins since they stay on Google’s servers for up to 30 days.\textsuperscript{285}

Finally, the Court of Appeals found that Google also violated authors’ moral rights in terms of paternity right and the integrity of the work. Firstly, if a quotation right had been available for Google it would have had to mention the names of the authors of the articles\textsuperscript{286} both in the search results, where the article texts were displayed in part, and on the web pages, where the article texts were displayed in whole. Authors’ moral rights were also violated in respect of the integrity of the work, because reproducing only an excerpt of the work changed the work.\textsuperscript{287} The Court noted that the authors had not given their consent to publish their works in a shortened form.\textsuperscript{288}

3.1.2. Framing and Inlining

The previous sub-section discussed copyright liability in hyperlinking. We will now investigate whether two additional forms of linking, namely, framing and inlining can result in copyright infringement.

Framing is a form of linking, where a website operator incorporates third party content on its own web page in a manner that creates an appearance of a unitary whole. While in hyperlinking the service provider essentially posts URL addresses to content, in framing the original content or a part of the original content is visible or audible already on the service provider’s web page. When the service user clicks on the framed

\begin{footnotesize}
\begin{enumerate}
\item Google Inc. v. Copiepresse R.no. 2011/2999, No. 817 at 32, 33, 35
\item In copyright law, the press is afforded a right to make quotations, to critique a work in a form of a press review and to report a topical event in a form of a news report.
\item Cf. Google Inc. v. Copiepresse R.no. 2011/2999, No. 817 at 32
\item Id. at 37
\item Id. at 34
\item Id. at 42
\item Id. at 42
\end{enumerate}
\end{footnotesize}
content, the embedded link directs her to the web page from where the content originates. Alternatively, she can view or listen to the content on the service provider’s web page. For instance, if you click on a YouTube video link that a friend has posted on your Facebook newsfeed, you can choose to watch the video in a small size frame without leaving the Facebook page or you can enter the YouTube page.

Inline linking or inlining is framing in the context of using image links. Inlining “allows one to import a graphic from a source website and incorporate it in one’s own website, creating the appearance that the in-lined graphic is a seamless part of the second web page.” Thumbnails are an example of commonly used inline image links. A thumbnail is a miniature image of an original bigger-sized picture.

The problem with framing and inlining is that an end-user might mistakenly think that the originator of all the content on the web page she is using is the service provider, whose website she has entered. This could trigger a trademark dispute, because it could be argued that a web page using framing misleads users with regard to the origins of the content. Also, framing and inlining could result in a moral rights or an adaptation rights dispute, because a framed site changes the appearance of the content retrieved from other sites. Further, a right holder could argue that framing or inlining creates an impression that she endorses or voluntarily chooses to associate herself and her works with the service provider who has framed her content.

In 2002, professional photographer Leslie Kelly sued Arriba Soft Corp. in the United States for direct infringement on the basis of illegally displaying his photographs as thumbnails among search results. Arriba operated an advertisement-funded search engine, which displayed search results in the form of images. Its web crawler software searched for full-sized originals on the Internet, downloaded them onto Arriba’s servers and created low-resolution thumbnails after which the full-sized originals were deleted from the servers. When the user clicked on the low-resolution thumbnail she could view the original full-sized version of the photo that was retrieved from the source website belonging to Kelly. Users were also allowed to copy the

---

289 Kelly v. Arriba Software, 280 F.3d 934 (9th Cir. 2002)
290 Fitzpatrick (2013)
291 Kelly v. Arriba Software, 280 F.3d 934 (9th Cir. 2002)
292 Id.
293 Id.
294 Id.
thumbnails onto their computers as low-resolution images. Any effort to enlarge the images resulted in a loss of clarity of the images.

The Court of Appeals ruled that Arriba’s use of thumbnails was transformative and hence fair use. The Court clarified that the thumbnails had a different function on the market than images residing on Kelly’s website, and hence, the market for Kelly’s images or the value of his images were not harmed.

“Kelly's images are artistic works intended to inform and to engage the viewer in an aesthetic experience. [...] Arriba's use of Kelly's images in the thumbnails is unrelated to any aesthetic purpose. Arriba’s search engine functions as a tool to help index and improve access to images on the internet [...] In fact, users are unlikely to enlarge the thumbnails and use them for artistic purposes because the thumbnails are of much lower-resolution than the originals; any enlargement results in a significant loss of clarity of the image, making them inappropriate as display material.”

In other words, Arriba did not compete with Kelly. On the contrary, the Court perceived Arriba’s service to improve the efficiency of image search on the Internet, which could increase Kelly’s chances of licensing or selling rights to his images.

In Perfect 10, Inc. v. Google, Inc., an American Court of Appeals came to similar conclusions. Perfect 10 sued Google claiming that Google Image Search infringed its copyrights by distributing thumbnail versions of Perfect 10’s images. The Court found that inline links did not infringe Perfect 10’s rights to control the display and distribution of works. Judge Ikuta noted that inline linking and framing could give the impression that Google showed the images within its web page but “the Copyright Act, unlike the Trademark Act, does not protect a copyright holder against acts that cause consumer confusion”. The Court found that the use of thumbnails was fair use, because Google’s use was highly transformative. Further, Google could not violate

---

295 Kelly v. Arriba Software, 280 F.3d 934 (9th Cir. 2002)
296 Id.
297 Id. at 20
298 Id. at 19
299 Id. at 8
300 Id. at 19
301 Cf. Perfect 10 Inc. v. Amazon.com, Inc. & Google, Inc., 487 F.3d 701 (USCA, 9th Cir. 2007)
302 Id.
303 Id. at 717
304 Id. at 721
the distribution right of Perfect 10, because it did not store copies of the original photos and hence it could not communicate them.\textsuperscript{305}

Courts in Germany have lately delivered contradicting opinions on framing and inlining, creating legal uncertainty.\textsuperscript{306} In 2011, the Court of Appeals of Düsseldorf\textsuperscript{307} ruled that the use of inlined photographs on a website constitutes making available to the public.\textsuperscript{308} In the case, an author of a blog used two photographs he had found on the Internet by embedding them into one of his blog entries.\textsuperscript{309} The author of the photographs sued, because he had not granted permission to use the photos.\textsuperscript{310} The Court reasoned that inline linking in this case constituted unauthorised making available to the public, because when the author of the blog made the photos visible on his website, he provided access to a new public, which the author of the photographs had not planned to direct his photographs for.\textsuperscript{311}

A half a year later the Court of Appeals of Cologne\textsuperscript{312} came to an opposite conclusion. It held that providing access to content by using framing did not constitute communication to the public.\textsuperscript{313} The Court argued that a prerequisite for ‘communication to the public’ to occur was that there was a certain level of control over the access to the protected works on the part of the communicator.\textsuperscript{314} The Court noted that in this case it was the originator of the works, not the framer, who controlled whether the content was communicated or not.\textsuperscript{315} In addition, the Court confirmed the view that framing simplifies the process of accessing content on the Internet\textsuperscript{316} and hence it should not be illegalised as such. An influencing factor in the opinion of the Court was that the framer did not try to pass the content as its own.\textsuperscript{317}

\textsuperscript{305} Perfect 10, Inc v. Amazon.com, Inc. & Google, Inc., 487 F.3d 701 (USCA, 9th Cir. 2007) at 717
\textsuperscript{306} Rauer (2013)
\textsuperscript{307} Cf. Decision Az. I-20 U 42/11, 8 October 2011, Düsseldorf Court of Appeal
\textsuperscript{308} Lovells & Petersenn (2012)
\textsuperscript{309} Id.
\textsuperscript{310} Id.
\textsuperscript{311} Id.
\textsuperscript{312} Decision Az. 6 U 206/11, 16 March 2012, Cologne Court of Appeal
\textsuperscript{313} Rauer (2013)
\textsuperscript{314} Id.
\textsuperscript{315} Id.
\textsuperscript{316} Id.
\textsuperscript{317} Id.
3.1.3. Conclusions

What have we learned from the previous cases about hyperlinking? The court decisions in 

napster.no\textsuperscript{318} and Paperboy\textsuperscript{319} present a view according to which hyperlinking does not constitute making works available to the public. The Paperboy decision also suggests that using snippets of copyrighted works in links does not infringe copyright if the snippets form an insubstantial part of the original work. Consequently, embedding substantial parts of source works in links or search results can be a breach of copyright.\textsuperscript{320} The Newsbooster decision\textsuperscript{321} suggests that collections of article headlines and article texts can be afforded database protection. Using substantial parts of a copyrighted database would therefore infringe copyright.

What about the dos and don’ts of framing and inlining? To avoid copyright liability the service provider should not store source works in their original form on its servers. Also, the technical quality of the framed content should be inferior compared to the original material. This way the service provider could, at least in the United States, succeed in proving that her use is fair use, because she is not competing with the original author in the same market. An American court could even find that the framing party’s re-use of works could create new business opportunities for the original author.

The service provider could also reduce legal risks by publishing the name of the author in connection with the framed content, as this would indicate that she respects the author’s moral rights and does not try to pass off the content as her own. In Europe, identifying the source could however make things worse. The 2011 decision of the Court of Appeals of Düsseldorf\textsuperscript{322} suggests that finding a new audience for a work, i.e. not competing in the same market, could incriminate the framing party if the author has not intended to direct her work to the new market. This logic derives from the droit d’auteur tradition of moral rights, on the basis of which an author can be granted pervasive rights to decide on the fate of her works. If her name and work were communicated to an audience she has not approved, the framing party could be found liable for infringing the author’s moral rights.

\textsuperscript{318} TONO mfl, EMI Norsk AS mfl mot A. 27.01.2005, HR-2005-00133-A (sak nr. 2004/822)
\textsuperscript{319} Holtzbrinck v. Paperboy I ZR 259/00 (17 July 2003) [2005] ECDR (7) 67, 77
\textsuperscript{320} Cf. Google Inc. v. Copiepresse R.no. 2011/2999, No. 817
\textsuperscript{321} Danske Dagblades Forening v. Newsbooster Aps, sag nr. FS F1-8703/2002
\textsuperscript{322} Decision Az. I-20 U 42/11, 8 October 2011, Düsseldorf Court of Appeal
3.2. LEGITIMACY OF FILE SHARING SERVICES

Online service providers, who copy, store, or distribute content for end-users or allow end-users to perform those operations themselves risk becoming liable for direct or indirect (secondary) copyright infringement. Direct liability can be harder for plaintiffs to prove. It can emerge in situations where the service provider does not qualify for ISP safe harbours and where it itself copies, distributes or modifies content without the permission of rights holders.

However, in an online environment it is most often the end-user who violates the reproduction or communication rights of authors. The service provider merely provides the means and technology that allow or induce the service user to infringe. When a service provider facilitates copyright infringement for an end-user it can become liable for indirect copyright infringement.

In some circumstances, the technology that the service provider uses in carrying out its online service can contribute to the emergence of copyright liability. In the following sections we will examine how new technologies have challenged the value creation logic of rights holders and how they in turn have challenged the technology developers’ and users’ right to use such technologies. We will start with two classic cases from the 1970’s and 1980’s that form a basis for a defence for many online service providers fighting for their existence in courts.

3.2.1. Pre-Internet Era: Sony Betamax and Amstrad

The case Sony Corp. of America v. Universal City Studios Inc. (hereafter ‘Sony Betamax’) dates back to 1976, when Universal Studios and its co-plaintiff Walt Disney Company sued Sony for manufacturing Betamax video tape recorders (Betamax VTRs), which enabled consumers to make unauthorised copies of copyrighted programmes which had been broadcasted on television.\(^2\) Universal and Disney asked the Court to decide whether Sony as a seller of home copying equipment violated the copyrights of Universal and Disney and whether Sony could be held liable for the

\(^2\) Sony Corp. of America v Universal City Studios Inc. 464 U.S. 417 (1984) at 2
alleged copyright infringements of consumers. Sony defended its case by asserting that its Betamax technology had many non-infringing uses and that using a timer for time-shift copying was fair use, because the use was private and non-commercial.

In 1979, the District Court dismissed the claims of Universal and Disney and ruled in favour of Sony. Universal and Disney appealed and in 1981 the Court of Appeals reversed the judgment in favour of Universal and Disney. The case worked its way to the Supreme Court, which in 1984 reversed the ruling of the Court of Appeals. The Supreme Court opined that the scope of the statutory monopolies of Universal and Disney could not be enlarged to encompass control over Sony’s Betamax technology, because such an expansion of copyright protection would be beyond the limits of copyright authorised by Congress. Further, Sony could not be held liable for indirect infringement. The Court stated “the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes.” The Supreme Court also considered that Universal and Disney did not succeed in proving that “time-shifting”, i.e. the practice of recording a programme that the consumer cannot view when it is televised and watching it later, impaired the commercial value of their copyrights or created a likelihood of future harm. On the contrary, the Court noted that time-shifting enlarges the television viewing audience.

According to Professor Pamela Samuelson “[t]he most obvious and most commercially significant legacy of Sony is the safe harbour it established for technologies having or capable of having substantial non-infringing uses.” The Sony safe harbour acts as a default rule for limiting the liability of technology developers. The ruling has enabled the emergence and commercial success of technologies such as photocopiers, CD burners, CD ripping software, MP3 players, iPods, digital video recorders, and peer-to-

---

324 Ibid. at 1-2
326 Sony Corp. of America v Universal City Studios Inc. 464 U.S. 417 (1984) at 3
327 Id.
328 Id.
329 Id. at 4
330 Id. at 39
331 Id. at 4
332 Id.
333 Samuelson (2006), p. 120
334 Id. p. 128
peer technologies. Consequently, the *Sony Betamax* decision has had a profound impact on the perceived legality of private copying and the liability of ISPs.

The significance of the *Sony Betamax* ruling on private copying is based on the principle of “non-transformative reproduction of whole works”. Under *Sony*, personal uses such as backup copying and space-, platform-, format- and time-shifting can be argued to be fair use. ISPs can also use the “non-transformative reproduction” argument in defending the caching of files. Cached copies enable uses of content akin to the time-shifted access in *Sony*.

In addition, under *Sony* telecom operators and other ISPs can argue that they should not be held liable for transmitting infringing files of which they have no knowledge. Also, copying entire works can be deemed as fair use under *Sony* especially if the likelihood of harm to the market is diminutive.

Another landmark case is *Amstrad*, i.e. *CBS Songs Ltd v. Amstrad Consumer Electronics Plc*. The case was argued before the House of Lords (Supreme Court of the United Kingdom) in 1988. The case dealt with a conflict of interests between the record producer *CBS Songs* and the manufacturer of recording equipment *Amstrad*. *CBS Songs* claimed that *Amstrad* violated its copyrights by manufacturing, advertising and offering for sale twin deck tape recorders, which allowed consumers to record pre-recorded compact cassettes (C-cassettes) onto blank C-cassettes at high speed. *CBS Songs* argued that *Amstrad* “authorised the public to infringe their copyrights” and that they were “joint infringers with the public”. In delivering the unanimous judgement of the Supreme Court, Lord Templeman confirmed that *Amstrad* did not authorise infringement. He noted:

---

335 Samuelson (2006), p. 120
336 Samuelson (2006)
337 Id. p. 145
338 Id. p. 135
339 Id. p. 142
340 Id.
341 Id.
342 *CBS Songs Ltd v Amstrad Consumer Electronics Plc. [1988] AC 1013*
343 Id.
344 Cf. IPCass (2013)
345 Cf. *CBS Songs Ltd v Amstrad Consumer Electronics Plc. [1988] AC 1013*
346 IPCass (2013)
347 *CBS Songs Ltd v Amstrad Consumer Electronics Plc. [1988] AC 1013*
“No manufacturer and no machine confers on the purchaser authority to copy unlawfully. The purchaser or other operator of the recorder determines whether he shall copy and what he shall copy. By selling the recorder Amstrad may facilitate copying in breach of copyright but do not authorise it.”

The Court further supported the interpretation that Amstrad was not a “joint infringer with the public.” According to Lord Templeman:

"[I]n the present case Amstrad do not procure infringement by offering for sale a machine which may be used for lawful or unlawful copying and they do not procure infringement by advertising the attractions of their machine to any purchaser who may decide to copy unlawfully. [...] The purchaser will not make unlawful copies because he has been induced or incited or persuaded to do so by Amstrad. The purchaser will make unlawful copies for his own use because he chooses to do so. Amstrad's advertisements may persuade the purchaser to buy an Amstrad machine but will not influence the purchaser's later decision to infringe copyright."

### 3.2.2. **Challenges of YouTube**

A service provider operating on the Internet can choose to build its service on a client-server or peer-to-peer (P2P) platform. Despite its bad reputation, running a business on a P2P platform is not any riskier than operating on a client-server platform. This becomes apparent when we examine the current challenges of the video hosting service YouTube and of notorious P2P services.

The majority of online media service providers run their business on a client-server platform. YouTube is no exception. In a client-server network, computers specialise to perform dedicated functions. Depending on the purpose of the computer it is either called a 'client' or a 'server'. For instance, if you are now reading this report on your computer and you have not downloaded the report yet, your computer performs the tasks of the client. The computer of the library (or any other service provider or individual) on which this report is stored operates as a server. Several software

---

348 CBS Songs Ltd v Amstrad Consumer Electronics Plc. [1988] AC 1013
349 Id.
350 Mitchell (n.d. a)
351 Id.
applications on your client computer, such as network software applications, browser applications, and reader applications, are needed for you to be able to access and read the report. The same applies to the server computer. The software applications of the server computer allow it to store the report and you to find and access the report. It may even permit you to download the report if the report is not copy-protected. If it were copy-protected with technological protection measures (TPMs) the copy protection would be established with a software application.

Client-server networks are centralised systems where the server processes all transactions among clients. Because of the centralisation of communication, it is easier for the service provider to organise data security, TPMs, and monitoring functions. The downside of a client-server network is that if the server crashes as a consequence of a technical problem, client computers lose their access to the service. Consequently, should a court issue an injunction on the service provider or order a seizure of the service providers’ servers, the service would cease to exist.

YouTube is a Google-owned video hosting website, which allows users to stream other users’ videos, and upload and share one’s own videos. YouTube’s Terms of Service prohibit downloading, copying, storage, and re-distribution of extant YouTube content. Also, the circumvention of technological protection measures and the manipulation of service functionality by any technological means are prohibited. Further, the copying, reproduction, distribution, transmission, broadcasting, display, selling, and licensing of third-party content without a prior written consent of YouTube or respective rights holders is prohibited. YouTube uses automated systems, such as ContentID to identify, remove and block infringing content. Also, rights holders can submit copyright infringement complaints on YouTube’s website.

YouTube service users do not pay for using the service. YouTube generates revenue from advertising. It compensates rights holders by paying a share of its advertising revenue. Service users can monetise their own videos by allowing advertisements to appear in connection to their videos.

352 Electric Communities (n.d.)
353 YouTube (2010), 5.1[L]
354 Id. 5.1[D]
355 Id. 5.1[C][G][H]
356 Id. 5.1[M]
357 See: YouTube (2013)
358 YouTube (n.d.)
Despite the prohibitions imposed on service users, plenty of unauthorised content circulates on YouTube’s website. As a consequence, YouTube has been under continuous attack from rights holders. Usually, YouTube’s defence strategy is based on a claim that it as a hosting service is protected from copyright liability on the basis ISP safe harbour provisions. In order to be able to qualify for the hosting service safe harbour it has to be able to prove that it does not have actual knowledge of illegal activity or information and that it upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.359

In Germany, the performance rights organisation GEMA sued YouTube in 2010360 for direct and indirect copyright infringements on the basis of unauthorised content that service users had shared on the website.361 In 2012, the Regional Court of Hamburg denied GEMA’s claim for direct infringement but found that YouTube was liable for indirect copyright infringement.362 The Court based its decision on the German doctrine of ‘interferer liability’ (Störerhaftung).363 Interferer liability arises when a service provider is liable for contributing causally to infringements.364 The Court opined that YouTube had not done enough to stop the infringing activities and it had taken too long to remove unauthorised content after YouTube had been informed about the infringements.365 The Court ordered YouTube to install additional keyword filters that would detect when users tried to upload infringing content.366 Both the parties have appealed to the Higher Regional Court in Hamburg.367

The issue of how diligently YouTube should monitor and remove content from its website has also been questioned in Viacom v. YouTube.368 Since 2007 the case has been transferred back and forth between the District Court and the Court of Appeals in the United States.369 The most urgent matter in which the disputing parties and the District Court and the Court of Appeals seem to disagree is whether YouTube is eligible for hosting service safe harbour protection.370 Viacom has tried to break YouTube’s

---

360 GEMA v. YouTube, Az. 310 O461/10, April 20, 2012
361 TTLF (n.d.)
362 Digital Civil Rights in Europe (2012)
363 GEMA (2013)
365 Digital Civil Rights in Europe (2012)
366 Id.
367 GEMA (2013)
368 Viacom International Inc. v. YouTube Inc. 07 Civ. 2103
369 Cf. Viacom International Inc. v. YouTube Inc., 676 F.3d 19, 42 (2d Cir. 2012)
370 Id.
defence by arguing that the employees of YouTube in fact have knowledge or awareness of specific infringing video clips.\textsuperscript{371} Viacom claims that since YouTube has knowledge and it has chosen not to remove infringing video clips it is facilitating access to infringing content.\textsuperscript{372} Viacom argues that as a consequence of the failure to remove infringing content YouTube cannot be afforded ISP safe harbour protection.\textsuperscript{373}

In 2012, the Court of Appeals affirmed Viacom's finding that YouTube indeed had actual knowledge of a handful of specific infringing video clips,\textsuperscript{374} which it had not removed from the service. The Court of Appeals returned the case back to the District Court asking it once again to decide whether (1) YouTube had knowledge or awareness of any specific copyright infringing content on its website, (2) YouTube wilfully blinded itself to such specific infringements, and if (3) YouTube had the right and ability to control infringing activities taking place on its website.\textsuperscript{375} The fourth question referred to the District Court concerned YouTube's content syndication software, which facilitates the syndication of YouTube videos to third parties. According to Viacom the syndication software and the agreements with third parties are yet another proof in that YouTube does not qualify for ISP safe harbour protection, because it uses infringing content in syndication for its financial benefit.\textsuperscript{376}

In April 2013, the District Court found for the second time, on all accounts, that YouTube is protected under the safe harbour provisions.\textsuperscript{377} In July 2013, Viacom filed its second appeal in the Court of Appeals.\textsuperscript{378} Three prominent American copyright scholars support Viacom's appeal, stating in their amicus brief (a legal opinion submitted to the court as a support for the decision) that several copyright rules support the secondary liability of YouTube. They note that the Court of Appeals should in its decision take into account that the legal responsibility of preventing, limiting, or eliminating harm rests on the party best able to do so,\textsuperscript{379} which in this case is YouTube.

\textsuperscript{371} Viacom International Inc. v. YouTube Inc., 676 F.3d 19, 42 (2d Cir. 2012)
\textsuperscript{372} Viacom International Inc. v. YouTube Inc. 07 Civ. 2103
\textsuperscript{373} Viacom Int’l Inc. v. YouTube Inc., 676 F.3d 19, 42 (2d Cir. 2012), Viacom International Inc. v. YouTube Inc. 07 Civ. 2103
\textsuperscript{374} Viacom Int’l Inc. v. YouTube Inc., 676 F.3d 19, 42 (2d Cir. 2012)
\textsuperscript{375} Latham & Watkins (2013), p. 1
\textsuperscript{376} Cf. Viacom International Inc. v. YouTube Inc. 07 Civ. 2103
\textsuperscript{377} Latham & Watkins (2013), p. 1
\textsuperscript{378} Viacom (2013)
\textsuperscript{379} Cass et al. (2013), p. 3
3.2.3. Notorious P2P Services

On a P2P network, every computer is equal and can communicate with any computer that it has rights to access. The computers of a P2P network are referred to as “peers” and they all can act as servers. Consequently, P2P networks are decentralised systems, where data security, TPMs, and content monitoring are harder to organise. In order for a P2P network to function, each participating computer needs to use the same networking protocols and software. The service provider or its affiliate provides the software usually free of charge.

In a simplified client-server network, the user would look for the desired file on one server. On a P2P network, the user searches for the file on all the computers that use the same P2P software. This is generally considered to be one of the strengths of P2P networks, as the feature allows networks to handle high volumes of file sharing traffic by distributing the workload across several computers. “Unlike the client-server model in which performance degrades with more users,” on a P2P network more users equals with efficiency, because the more users make a particular file available from their computers, the easier it is for other users to acquire that file. This is also why P2P networks are more flexible than client-server networks when a server or network failure occurs. Even if several computers were eliminated, it would be likely that the service could continue to exist.

Consequently, P2P networks offer a challenge for law enforcement officials, because an injunction or a seizure of a number of servers does not necessarily stop infringing activities. This is why rights holders have lately asked courts to issue orders that enjoin Internet access operators (often telecom operators), which are in the best position to prevent, limit, or eliminate infringing activities, to use IP address or DNS blocking technologies to prevent access to infringing sites.

---

380 Bestofmedia Team (2011)
381 Carmack (n.d.)
382 Bruce (2012)
383 Mitchell (n.d. b)
384 Id.
385 Bruce (2012)
386 Mitchell (n.d. b)
387 Andy (2013)
P2P technologies deployed by file sharing services are usually hybrid designs.\(^{388}\) All P2P solutions are, however, based on the idea that the computers of the service provider do not store or rely on media files. Media files reside on the hard drives of service users. In the first generation P2P networks, service providers hosted central servers to perform search and indexing functions.\(^{389}\) The indices conveyed information about what content was available on the network and where it could be found. The computers of service users maintained indices of the files that they made available to other network users.\(^{390}\)

In more advanced P2P solutions, any computer on the network can function as a central indexing server (‘supernode’) if it meets the technical requirements.\(^{391}\) When a user makes a search request, it is sent to all computers that are connected with it, which in turn pass the request along to other connected peers.\(^{392}\)

BitTorrent systems go one step further. Instead of copying the whole file from one computer, your computer downloads the file from multiple peer computers in small pieces,\(^{393}\) which are re-assembled together on your computer.\(^{394}\) This is why BitTorrent allows faster download speeds of large media files. A specialty of the BitTorrent system is that the more you share with others, the faster your downloads become.\(^{395}\) In addition, the system does not allow you to be only a downloader; you also have to share.\(^{396}\) In other words, the BitTorrent software forces users to become distributors if they want to use the service for downloading content.

P2P technologies seem to be gaining a foothold not only in rogue services but also legitimate services. For instance, Spotify deploys BitTorrent with the aim to use less servers, less bandwidth and achieve better up-time.\(^{397}\)

\(^{388}\) Mitchell (n.d. b)

\(^{389}\) Cf. Mitchell (n.d. b), Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd, 380 F. 3d 1154 (9th Cir. 2004)

\(^{390}\) Id.

\(^{391}\) Id.

\(^{392}\) Id.

\(^{393}\) Bruce (2012)

\(^{394}\) Carmack (n.d.)

\(^{395}\) Id.

\(^{396}\) Id.

\(^{397}\) Ernesto (2011)
3.2.3.1. Napster

One of the first widely available implementations of P2P services was Napster.\footnote{Bruce (2012)} It was also one of the first P2P services taken to court. In short, the service worked as follows:

“A central database held information about all the music files held by members; when you searched for a song to download, you would actually be connecting to another online user and downloading from them. In turn, once you had that song in your Napster library, it would be available as a “source” for others on the network. You could also just add your own files, which would then be indexed and added to the database, ready to propagate across the world.”\footnote{Id.}

In 2000, A&M Records sued Napster for indirect copyright infringement arguing that Napster’s users were engaged in a wholesale reproduction and distribution of copyrighted works constituting a direct infringement.\footnote{A&M Records Inc. v. Napster Inc. 239 F.3d 1004 (9th Cir 2001) at 1, 17} Napster argued that the use by its users constituted fair use in a form of sampling, space-shifting, and permissive distribution of recordings by both new and established artists.\footnote{Id. at 21} The Court accepted only ‘permissive distribution’ as fair use.\footnote{Id. at 19} By ruling out Napster’s defence the Court made it vulnerable for indirect infringement.

The Court went on assessing Napster’s secondary liability in terms of contributory and vicarious infringement. The Court determined that ‘contributory liability’ exists “if the defendant engages in personal conduct that encourages or assists the infringement.”\footnote{Id. at 48} In addition, “[c]ontributory liability requires that the secondary infringer know[s] or have reason to know of direct infringement.”\footnote{Id. at 50} The Court held that Napster had actual and constructive knowledge of the direct infringements.\footnote{Id. at 50} As a consequence Napster was found to be liable for contributory infringement.\footnote{Id. at 59}

With regard to ‘vicarious infringement’ the Court noted that Napster could be held liable if it had the right and ability to supervise infringing activities and also had a direct financial interest in such activities.\footnote{Id. at 60} The Court reaffirmed that Napster
financially benefited from the circulation of copyrighted works in its system. With respect to the right to supervise (“control”) the Court of Appeals stated that Napster “retains the right to control access to its system. Napster has an express reservation of rights policy, stating on its website that it expressly reserves the right to refuse service and terminate accounts in its discretion, including, but not limited to, if Napster believes that user conduct violates applicable law . . . or for any reason in Napster’s sole discretion, with or without cause.”

The Court noted that the ability of Napster to police the content of files was limited, because the system could only check that the file was in the required MP3 format. However, Napster had the ability to locate infringing materials on the basis of file names listed on its search indices. On the basis of all these premises the Court found Napster liable for vicarious infringement.

3.2.3.2. Grokster

The first precedent coming from the Supreme Court in the United States with regard to the legitimacy of P2P file sharing services was Metro-Goldwyn-Mayer Studios v. Grokster. In 2005, the Supreme Court held Grokster and its software provider StreamCast Networks liable for secondary copyright infringement, because there was evidence that Grokster and StreamCast intended to use the P2P software to infringe.

The technology that Grokster and StreamCast used was decentralised. Their servers did not intercept the content of search requests. Nor did the servers mediate file transfers conducted by service users. There was no central node. Communications was dispersed across the network between peer computers. As a consequence Grokster and StreamCast did not have knowledge when files were copied and which files were

---

408 A&M Records Inc. v. Napster Inc. 239 F.3d 1004 (9th Cir 2001) at 61
409 Id. at 63
410 Id. at 66
411 Id. at 67
412 Id. at 67
413 Metro-Goldwyn-Mayer Studios Inc. v Grokster Ltd 545 U.S. (2005)
414 Id.
415 Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd, 380 F. 3d 1154 (9th Cir. 2004)
416 Id.
417 Id.
418 Metro-Goldwyn-Mayer Studios Inc. v Grokster Ltd 545 U.S. (2005), p. 4
copied. However, the software allowed to identify what content was available within the network.\textsuperscript{419} Hence, it also allowed the identification of infringing content. This made it possible for the plaintiffs to prove that the service was used for illegal activities.

StreamCast also monitored the number of users downloading its software.\textsuperscript{420} In addition, it monitored the number of music files that the service users downloaded.\textsuperscript{421} Further, internal firm documents and promotion materials revealed that both StreamCast and Grokster sought to attract former Napster users.\textsuperscript{422} Both the firms also generated income by selling advertising space on their websites.\textsuperscript{423} Finally, there was no evidence that either company made any actual effort to filter and remove infringing content or otherwise impede the sharing of copyrighted works.\textsuperscript{424} The Court noted:

\begin{quote}
\textit{“Although Grokster appears to have sent e-mails warning users about infringing content when it received threatening notice from the copyright holders, it never blocked anyone from continuing to use its software to share copyrighted files.”}\textsuperscript{425}
\end{quote}

The Supreme Court ruled against Grokster and StreamCast despite the fact that their software also had substantial non-infringing uses.\textsuperscript{426} Three incriminating factors sealed the firms’ fate: (1) both companies were active in promoting their service to a market, which already was susceptible to distributing illegal content, (2) both companies generated income from the illegal activities of service users, and (3) neither of the companies did enough to prevent users from committing copyright infringements.

\subsection*{3.2.3.3. Kazaa}

In the Netherlands, the Dutch music rights organisation Buma/Stemra initiated a lawsuit against Kazaa B.V. in 2001.\textsuperscript{427} The case worked its way through to the Supreme Court, which in 2003 upheld the decision of the Amsterdam Court of Appeals stating that the software of Kazaa, which was identical with the software of Grokster, did not

\footnotesize{\textsuperscript{419} Metro-Goldwyn-Mayer Studios Inc. v Grokster Ltd 545 U.S. (2005), p. 4
\textsuperscript{420} Id. p. 6
\textsuperscript{421} Id.
\textsuperscript{422} Id. pp. 6-7
\textsuperscript{423} Id. p. 8
\textsuperscript{424} Id. pp. 8-9
\textsuperscript{425} Id. p. 9
\textsuperscript{426} Smith (2011), p. 1566-67
\textsuperscript{427} Vereniging Buma and Stichting Stemra v Kazaa B.V. AN7253 Case no.: C02/186HR}
raise indirect copyright liability. The Supreme Court also rejected Buma/Stemra’s request for that Kazaa should modify its software in order to reduce the amount of infringing content in the service.

The decision of the Supreme Court of the Netherlands is one of the very few in which a P2P file sharing service has been able to escape liability. However, the Supreme Court of Netherlands did not address the merits of the case in their entirety. It left important questions unanswered, such as what constitutes facilitation of copyright infringement on the part of a service provider.

Two years later, the new owner of Kazaa, Sharman License Holdings, was in trouble in Australia, where Universal Music Australia sued it and its affiliates on the grounds of direct copyright infringement by communicating sound recordings unlawfully to the public and authorised copyright infringement by authorising users to make unauthorised copies of recordings, which they communicated unlawfully to the public. The Federal Court of Australia narrowed down the petition by dismissing the claim of direct liability. In deciding on the authorisation of copyright infringement (indirect liability), the Court revisited, among others, the court decisions in Amstrad and Moorhouse. The Court opined that Kazaa could not be held liable for authorised copyright infringement "merely because it provides the facilities". It also argued that communicating content by sharing files on the Internet does not constitute a broadcasting service within the meaning of the Australian Broadcasting Services Act.

---

428 Mazziotti (2008), p. 163; Evers (2003). See also: Vereniging Buma and Stichting Stemra v Kazaa B.V. AN7253 Case no.: C02/186HR
429 Mazziotti (2008), p. 163
430 Id.
431 Universal’s claims included the marketing, offering, and supplying Kazaa software; developing, maintaining the Kazaa software; developing, maintaining, and making available technical features, resources and information including indexes and supernodes required in the operation of the Kazaa software; establishing, operating, and maintaining the infrastructure used in the operation of Kazaa software; and establishing, operating, and maintaining websites and services related to Kazaa software. See Universal Music Australia Pty Ltd. v. Sharman License Holdings Ltd [2005] FCA, §33 and §37
432 Universal Music Australia Pty Ltd. v. Sharman License Holdings Ltd [2005] FCA § 34-35, § 37
433 Id. §362
434 CBS Songs Ltd v Amstrad Consumer Electronics Plc. [1988] AC 1013
435 See: University of New South Wales v Moorhouse [1975] HCA 26. In the case, Mr Moorhouse accused University of New South Wales of infringing his copyrights by reproducing or authorising the reproduction of parts of his book in a material form, without a license, by allowing individuals to photocopy books with photocopying machines located in the university’s library (see HCA 26 (1975) at 3).
436 Universal Music Australia Pty Ltd. v. Sharman License Holdings Ltd [2005] FCA, §401
437 Id. §362
The Court directed its attention to finding out whether *Sharman* had knowledge of the infringing activities, whether it sanctioned, countenanced or approved infringements, or whether it had a power to control and prevent the infringements.\textsuperscript{438} The conclusion was that *Sharman* was liable for authorising the making of copies and communication of sound recordings.\textsuperscript{439} The liability arose on three grounds. Firstly, the Court noted:

“[D]espite the fact that the Kazaa website contains warnings against the sharing of copyright files, and an end user licence agreement under which users are made to agree not to infringe copyright, it has long been obvious that those measures are ineffective to prevent, or even substantially to curtail, copyright infringements by users. The respondents have long known that the Kazaa system is widely used for the sharing of copyright files [...]”\textsuperscript{440}

Secondly, the Court acknowledged that there were filtering technologies that *Kazaa* could have used to make it difficult for service users to search for infringing content.\textsuperscript{441} However, because *Kazaa* was financed by advertising revenue, it was “in the respondents’ financial interest to maximise, not to minimise, music file-sharing”.\textsuperscript{442}

Thirdly, *Kazaa* incriminated itself with its website, in which it encouraged service users to increase their file sharing and join the “Kazaa Revolution” against record labels.\textsuperscript{443} The Court held that to the young audience, which were the predominant users of Kazaa, the effect of the web page “would be to encourage visitors to think it [is] ‘cool’ to defy the record companies by ignoring copyright constraints”.\textsuperscript{444}

As a result, the Court granted an injunction requiring *Sharman* to add content filtering features to *Kazaa*.\textsuperscript{445} The Court proposed two alternatives: (1) an adoption of a new technology in a form of a non-optional keyword filtering software that would exclude unauthorised works from search results or (2) a modification of an existing Kazaa TopSearch software to limit search results to licensed works.\textsuperscript{446}

\textsuperscript{438} Cf. Universal Music Australia Pty Ltd. v. Sharman License Holdings Ltd [2005] FCA § 366-386
\textsuperscript{439} Id. p. 6
\textsuperscript{440} Id. p. 4
\textsuperscript{441} Id.
\textsuperscript{442} Id. p. 5
\textsuperscript{443} Id.
\textsuperscript{444} Id.
\textsuperscript{445} Id. § 520
\textsuperscript{446} Id. p. 7
According to Seng, the Federal Court of Australia created in Kazaa a situation where ‘authorisation of copyright infringement’ becomes an issue of software design. The service provider’s failure to take preventive measures by using filtering technologies leaves the service provider vulnerable for indirect copyright liability. Seng criticises the decision, because the Court did not take into account the fact that filtering technologies often are inefficient and generate false positives and false negatives. The filtering systems are prone to filter out authorised content and allow infringing content to pass through. Apart from an automated system, manual labour would be needed to sort out the false positives and negatives. Also, a defective technology could, at least in principle, make the service provider liable for not only indirect copyright infringement but also other violations such as hindering free speech or breaching user contracts.

After the rulings of U.S. Supreme Court in Grokster and Australian Supreme Court in Kazaa, which both found the P2P service providers liable for indirect copyright infringement, Sharman settled with American rights holders in 2006. Sharman agreed to pay $100 million in damages to record labels and an undisclosed sum to film studios with an affirmation to commit to develop the service to become fully legal.

### 3.2.3.4. The Pirate Bay and Finreactor

Perhaps the best-known BitTorrent file sharing service in the world is the Swedish The Pirate Bay (hereafter ’TPB’). In 2010, Svea Court of Appeals found the co-founders of TPB liable for criminal copyright infringement for assisting in copyright violations. The Svea Court of Appeals upheld the decision of the District Court to sanction the founders with imprisonment and monetary damages. However, it reduced the prison sentences to 4-10 months (depending on the defendant) and increased the monetary fines to constitute about €5 million.

In Europe, the imprisonment of the founders of TPB and the amount of monetary damages gave rise to an avid debate about the proportionality of the penalties. When

---

447 Seng (2008), p. 14
448 Id.
449 Id.
449 Nguyen (2006)
450 Id.
452 Id.
the Supreme Court of Sweden (Högsta Domstolen) denied the appeal of TPB in 2012,\textsuperscript{453} two of the co-founders, Fredrik Neij and Peter Sunde Kolmisoppi, further filed a complaint to the European Court of Human Rights (ECtHR). They claimed that the rulings of the Swedish courts violated their freedom of expression.\textsuperscript{454} Freedom of expression is recognised as a fundamental human right in Article 10 of the European Convention of Human Rights (ECHR).\textsuperscript{455} Neij and Sunde Kolmisoppi argued that Article 10 of the “Convention enshrines the right to offer an automatic service of transferring unprotected material between users, according to basic principles of communication on [the] Internet, and within the information society” and that the “Convention protects the right to arrange a service on the Internet which can be used for both legal and illegal purposes”.\textsuperscript{456}

In the spring of 2013, ECtHR found that the prison sentences of TPB founders and award of damages were not disproportionate.\textsuperscript{457} ECtHR noted that the TPB founders had been indifferent with regard to the fact that copyright-protected works were circulating in their service, and despite having been informed about the infringing activities, they had not taken any action to remove infringing torrent files.\textsuperscript{458} In fact, TPB had been extremely impudent when responding to the takedown notices of rights holders. For instance, in their response to Dreamworks, TPB called the American film studio and their legal council “morons, who should sodomise themselves with retractable batons”.\textsuperscript{459} TPB’s letter ended with a greeting “Go fuck yourself”.\textsuperscript{460}

In its decision, ECtHR reasoned that the nature of information contained in the BitTorrent files and the founders’ indifference in removing infringing content justified the interference with their freedom of expression and that the interference was

\textsuperscript{453} Ricknäs (2012)
\textsuperscript{454} Fredrik Neij and Peter Sunde Kolmisoppi against Sweden, Decision, Application no. 40397/12, European Court of Human Rights, Fifth Section (2013)
\textsuperscript{455} Article 10 “Freedom of Expression” of the European Convention of Human Rights reads: [1] Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. [2] 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.
\textsuperscript{456} Fredrik Neij and Peter Sunde Kolmisoppi against Sweden, Decision, Application no. 40397/12, European Court of Human Rights, Fifth Section (2013)
\textsuperscript{457} Id.
\textsuperscript{458} Id.
\textsuperscript{459} Cf. Jokinen (2009), p. 12, Dennis (2011)
\textsuperscript{460} Id., Id.
necessary in a democratic society within the meaning of Article 10(2) of the ECHR. Consequently, ECtHR found the application of Neij and Sunde Kolmisoppi to be manifestly ill-founded and hence inadmissible.

At the same time with TPB trials, the legitimacy of the file sharing service Finreactor was tested in Finnish courts. Rights holders sued Finreactor initially in 2006. In 2012, the Supreme Court of Finland confirmed that the administrators of Finreactor were liable for unauthorised reproduction and communication of copyrighted works as co-infringers with service users. As there is no third party civil liability (indirect liability) in Finnish law, liability in civil cases is based on direct liability. If intermediaries are involved in a copyright infringement case, the court assesses the case “in its entirety”. Further, at the time of the Finreactor case, the rights holders could not accuse the administrators of Finreactor of criminal copyright infringement, because Finnish law then did not recognise criminal offence in cases in which the alleged infringer did not have a financial interest. Unlike the founders of TPB, who generated substantial revenues with the sale of advertisements, the administrators of Finreactor did not make money with their service. According to the Court, running the Finreactor service was a hobby for the defendants. Hence, the Finreactor administrators were sanctioned to pay monetary damages worth €421,780,00.

From the technical perspective the BitTorrent service of Finreactor was similar to TPB. Also, the defence strategies were identical: both Finreactor and TPB argued that no infringing files were transmitted through their servers but rather the end users reproduced the works. Finreactor and TPB also asserted that transmitting information about the location of works does not constitute copyright infringement. Further, both the defendants argued that ISP safe harbour provisions exempt them...

---

461 Fredrik Neij and Peter Sunde Kolmisoppi against Sweden, Decision, Application no. 40397/12, European Court of Human Rights, Fifth Section (2013)
462 Fredrik Neij and Peter Sunde Kolmisoppi against Sweden, Decision, Application no. 40397/12, European Court of Human Rights, Fifth Section (2013)
463 Finreactor KKO:2010:47
464 Finreactor KKO:2010:47 at 22
465 Oesch (2002), p. 115
466 Cf. Jokinen (2009), p. 10
467 Jokinen (2009), p. 11
469 Finreactor KKO:2010:47
470 Jokinen (2009), p. 10
471 Jokinen (2009), p. 10
from copyright liability.\textsuperscript{472} Neither the Supreme Court of Finland nor Svea Court of Appeals in Sweden accepted the defendants’ claims.

\subsection*{3.2.4. Cyberlockers at Bay}

Typically, a cyberlocker is a file hosting service provider that provides password-protected hard drive space\textsuperscript{473} for customers to store their data, text and media files. Examples of cloud services are Google Drive, SkyDrive, iCloud, and Amazon Cloud Drive. Individuals and firms can use these services, for instance, as an electronic archive to store backup copies of important files, as a shared working space for collaborative projects, or to substitute the transfer of files via email messaging. The servers of cyberlockers can also be used to run software applications that a customer does not have on her computer, and to run tasks for which the computer processor is too slow or there is not enough storage memory on the computer.\textsuperscript{474}

Cyberlockers are often referred to as cloud services. The term derives from cloud computing. Cloud computing is “\textit{a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction}.”\textsuperscript{475} In practical terms this means that the service provider hosts servers with accompanying software providing a varying array of functionality. The servers can reside anywhere in the world centralised on one location or dispersed on several locations. As a customer you can access your files residing on those servers with any device with an Internet connection and a web browser application. The system is automated to the extent that the service provider does not manually interfere with your communications with and within the system.

In a cloud system, a central server monitors and administers the traffic and client requests.\textsuperscript{476} When a client computer sends a request to access a file, the central server

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{472} Jokinen (2009), p. 12
\item \textsuperscript{473} Gil (n.d.)
\item \textsuperscript{474} Strickland (2013a)
\item \textsuperscript{475} Mell & Grance (2011), p. 2
\item \textsuperscript{476} Strickland (2013b)
\end{itemize}
\end{footnotesize}
forwards the client request to another server that houses the file. Cloud computing systems need at least twice the number of storage servers in order to keep clients’ information safely stored, as there always is a possibility that a server breaks down. Hence, the system automatically creates backup copies of files.

Typically, when you store a file on a cloud, an URL address or a hyperlink is created for the file. Your friends and colleagues can access the file if they know the URL or if they have an access to the hyperlink. Some systems allow you to protect your files with passwords. Obviously, then your friends and colleagues can access your files only if they in addition to knowing the URL or hyperlink also know your password.

For a cyberlocker copyright liability can emerge if a customer uploads, stores and shares copyrighted works for the use of which she does not have permission. If a customer merely uploads and stores an infringing file on a cyberlocker’s server it is likely that the infringement is not discovered, unless the cyberlocker is obligated to implement a filtering software, which has the capacity to identify and remove infringing files. However, usually indirect copyright liability emerges for the service provider when a customer shares an infringing file by communicating the corresponding URL or hyperlink to the public. Yet another matter are the backup copies that the system automatically creates in order to preserve customers’ files should a storage server break down. This could, at least in principle, facilitate the emergence of direct copyright liability on the part of the service provider.

The following analysis of a Supreme Court case in Germany sheds light on the monitoring obligations that courts might impose on cyberlockers. The decision of the Supreme Court in *Rapidshare v. Walther de Gruyter and Campus Verlag* (2013) is contrasted with two opposite opinions originating from the Court of Justice of the European Union (CJEU). The cases reveal that there is still great legal uncertainty involved in whether companies operating as hosting services can be subjected to monitoring obligations and what can be required of such monitoring software.

477 Cf. Strickland (2013a)
478 Id.
479 Id.
3.2.4.1. **Rapidshare v. Walther de Gruyter**

In August 2013, the Supreme Court of Germany (Bundesgerichtshof) found the cyberlocker *Rapidshare* liable as an indirect infringer ("Störer") for the infringements of service users on the grounds that *Rapidshare* had failed to fulfil reasonable examination obligations despite of having been in a position to prevent the infringements.\(^480\) Two book publishers, *Walther de Gruyter* and *Campus Verlag* had sued *Rapidshare* in 2010 for making their works publicly accessible and allowing others to make their works publicly accessible.\(^481\)

On the Rapidshare website, the user can upload files, which will then be stored on the service provider’s server.\(^482\) After uploading the file the user is provided with a download link via which she can retrieve and download the stored file on her computer.\(^483\) "*Rapidshare does not provide a table of contents of the uploaded files, nor a search function or other type of catalogue of these files.*"\(^484\) However, service users can place download links in other link libraries on the Internet through which third parties can access the stored files on *Rapidshare’s* servers.\(^485\)

*Rapidshare* offers a freemium and a premium account service. The freemium service can be used without registration.\(^486\) It offers restricted functionality: downloads are delayed, additional downloads are not possible immediately afterwards, the download speed is limited, and uploaded files cannot be downloaded more than ten times.\(^487\) The premium service requires registration and allows faster and simultaneous downloading of several files.\(^488\) At one stage *Rapidshare* awarded "premium points" to users whose uploaded files were retrieved by other persons.\(^489\) These points could be used to acquire various bonuses such as a free premium account.\(^490\) As of July 1st, 2010, *Rapidshare*, however, gave up the system of premium points.\(^491\) Instead, service users are now able

\(^{480}\) Rapidshare AG v. Walther de Gruyter GmbH et al., I ZR/79/12, August 15, 2013 at 59  
\(^{481}\) Id. at 5, 6  
\(^{482}\) Id. at 1  
\(^{483}\) Id.  
\(^{484}\) Id. at 2  
\(^{485}\) Id.  
\(^{486}\) Id. at 3  
\(^{487}\) Id.  
\(^{488}\) Id.  
\(^{489}\) Id. at 4  
\(^{490}\) Id. at 4  
\(^{491}\) Id. at 4
to purchase so-called “rapids” and a service package “PremiumPro”, which are substantially similar to the former premium account service.492

In the examination of Rapidshare’s involvement the Supreme Court noted that liability as an accomplice requires knowledge of a specific offence, and that it could not be assumed that RapidShare had such knowledge.493 Hence, indirect liability could not be established on these grounds. However, the Court opined that Rapidshare was in a position where it could monitor and examine traffic on its servers.494 Even though Article 15(1) of Directive 2000/31/EC495 exempts hosting services from general monitoring obligations, the Court concluded that monitoring obligations “in specific cases are not excluded”.496 With this the Court implied that when a service provider receives a specified list of infringing works497 in the form of a cease-and-desist letter the service provider gains specific knowledge on the basis of which it should be able to filter out the infringing files that the rights holder has specified. The Court did not take a stance, whether the sender of the cease-and-desist letter is obligated to inform the service provider of the specific locations of the infringing files on the Internet.

Further, the Court opined that service providers who store information provided by users are subjected to certain risks, which is why they are obligated to apply reasonable care and additional examination to detect and prevent unlawful activities.498 The Supreme Court noted that Rapidshare had increased the risk of user infringements with its own actions when providing premium points to users whose files were downloaded by third parties.499 In addition, allowing users to use the service anonymously increased the risk of infringement.500 It could also be established that Rapidshare had a financial interest in abetting users to seek mass downloads.501

The Court of Appeals had earlier suggested that a volume of 100,000 downloads for some files residing on Rapidshare’s servers could only be achieved with highly

492 Rapidshare AG v. Walther de Gruyter GmbH et al., I ZR/79/12, August 15, 2013 at 4
493 Id. at 23
494 Id. at 24
495 Article 15(1) of the E-Commerce Directive reads: “Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.”
496 Rapidshare AG v. Walther de Gruyter GmbH et al., I ZR/79/12, August 15, 2013 at 24
497 In the list, the rights holder lists works including their titles, of which it has evidence that they are distributed unlawfully on the Internet.
498 Cf. Rapidshare AG v. Walther de Gruyter GmbH et al., I ZR/79/12, August 15, 2013 at 26
499 Id. at 31, 36
500 Id. at 35
501 Id. at 34
attractive content, which most likely was unlawful content.\textsuperscript{502} The Supreme Court agreed noting that even though some companies might want to use Rapidshare’s service for the legitimate distribution of software updates intended for a large number of persons, the assumption that files with a high number of downloads most likely comprised unauthorised films, music or software, was only logical.\textsuperscript{503} Further, the Court considered that the service design of Rapidshare created a significant incentive for the users to exploit the service for massive rights infringements.\textsuperscript{504}

For the previous reasons, the Supreme Court ordered Rapidshare to install a keyword filtering system that comprehensively monitors link resources by searching in a targeted manner.\textsuperscript{505} The objective of the filtering system is to monitor links and accompanying texts in order to detect if they include titles or snippets of titles of copyrighted works.\textsuperscript{506} In addition, Rapidshare was ordered to use appropriate means, such as search requests and web crawlers, to search for infringing links directing traffic to Rapidshare’s service on search engines such as Google, Facebook, and Twitter.\textsuperscript{507}

The decision of the Supreme Court of Germany is particularly interesting with regard to the Court’s interpretation of Article 15 of the E-Commerce Directive. In its decision, the Supreme Court requires Rapidshare to search for infringing files independently and pre-emptively on the basis of titles of works, the information of which it has received from rights holders. Requiring a service provider to implement such a filtering system could be argued to constitute a “general monitoring obligation”. However, it seems that the Supreme Court assumes that using keyword filtering “in a targeted manner” constitutes “monitoring obligations in a specific case”,\textsuperscript{508} which would place the decision in compliance with the E-Commerce Directive. However, it could also be argued that the monitoring system suggested by the Court breaches Article 15.

In \textit{Scarlet v. SABAM (2011)},\textsuperscript{509} the European Court of Justice (CJEU) decided that Internet access providers cannot be ordered to install a filtering system to monitor all electronic communications and block content in order to protect IPRs.\textsuperscript{510} CJEU ruled

\begin{footnotesize}
\begin{enumerate}
\item Rapidehshare AG v. Walther de Gruyter GmbH et al., I ZR/79/12, August 15, 2013 at 33
\item Id.
\item Id. at 37
\item Id. at 54
\item Id.
\item Id.
\item See: Directive 200/31/EC, Preamble at 47
\item Scarlet Extended SA vs. SABAM, CJEU, Case C-70/10, November 24, 2011
\item Digital Civil Rights Europe (2011)
\end{enumerate}
\end{footnotesize}
that a filtering and blocking system for all customers for an unlimited time is a preventive measure, which violates fundamental rights, more particularly the right to privacy, freedom of communication, and freedom of information on the part of service users. In addition, it breaches the freedom of the ISP to conduct its business.

In a similar case, SABAM v. Netlog (2012), CJEU ruled that social networking sites are precluded from using preventive filtering. As in Scarlet v. SABAM, CJEU opined that requiring a hosting service to install a filtering system that monitors all or most of the information stored by the service provider for an unlimited time “would result in a serious infringement of the freedom of the hosting service provider to conduct its business since it would require [...] the hosting service provider to install a complicated, costly, permanent computer system at its own expense.”

Moreover, the effects would not be limited to the service provider, as the filtering system could infringe service users’ right to protect their personal data and freedom to receive or impart information. In the context of Neglog’s social networking service, a filtering system would involve the identification, systematic analysis, and processing of profile information. In addition, a filtering system could potentially undermine the freedom of information, since that system might not distinguish adequately between unlawful and lawful content, which in return could lead to the blocking of lawful communications. CJEU noted that national authorities and courts must strike a fair balance between the protection of intellectual property rights enjoyed by copyright holders and the freedom to conduct a business enjoyed by hosting service providers.

### 3.2.5. Conclusions

Online service providers are not usually found liable for copyright infringement on the grounds of merely providing the technology that allows end-users to commit copyright

---

511 Cf. Digital Civil Rights Europe (2011)
512 Digital Civil Rights Europe (2011)
513 SABAM v. Netlog, CJEU, Case C-360/10, February 16, 2012
514 Id. at 52
515 Id. at 45-46
516 Id. at 48
517 Id. at 49
518 Id. at 50
519 Id. at 44
violations. Case law suggests that liability emerges when a service provider fails to remove infringing content from its website. From this follows that in order to secure the legality of the service, the service provider must act expediently after receiving a takedown notice from a rights holder. A risk here is that if for some reason the takedown notice were inaccurate, the service provider might end up removing legitimate content. This could breach service users' fundamental rights.

The service provider must also be prepared to implement content filtering to identify and remove infringing content. Service providers that have been found liable for infringements have failed to police, or have chosen to ignore, infringing activities. It is noteworthy that copyright liability can emerge regardless whether the failure to monitor has been intentional or unintentional on the part of the service provider.

It seems that courts increasingly perceive ISPs to be in the best position to prevent, limit and eliminate harm occurring to rights holders. When an ISP chooses to integrate the production of UGC in its business model it is subjected to risks that traditional publishers can avoid. Some courts have held that for this reason ISPs are obligated to apply more vigorous examination measures to prevent unlawful activities. File hosting service providers are generally obligated to filter out infringing content while Internet access providers are increasingly required to block access to infringing websites.

According to law, ISPs are exempt from pre-emptive monitoring obligations. However, the findings of this thesis suggest that it is not exceptional that a court requires an ISP to implement content filtering. According to CJEU, Internet access providers and social networking sites can be exempt from pre-emptive monitoring obligations in the EU if the monitoring has a capacity to violate service users’ fundamental rights. However, these rulings do not imply that national courts could not impose monitoring obligations on ISPs at all. Nor do the rulings imply in any way that distributing unauthorised content could be deemed legal under the provisions of fundamental rights. The fates of the founders of The Pirate Bay also confirm this.

Article 15 “No General Obligation to Monitor” of the E-Commerce Directive limits the ability of the courts to impose monitoring obligations on ISPs. The problem in enforcing the rule is that there does not seem to be a common understanding of what differentiates a “general monitoring system” from a “non-general monitoring system”.
Nevertheless, when implementing content filtering, ISPs should take great care to avoid ancillary legal problems. Indeed, in the effort to avoid copyright liability, ISPs could risk becoming liable for violating the rights of consumers. Present-day content filtering systems are prone to filter out not only illegal content but also legal content. This could lead to a breach of the right to freedom of expression. The filtering mechanism may not be too intrusive either, as the ISP must be able to secure the privacy of service users.

The case studies indicate that technological solutions can contribute to the emergence of copyright liability. However, P2P technologies are not any riskier than client-server platforms. Hosting information about infringing files and hosting the actual infringing files can both lead to an indictment. What counts is how the ISP allows end-users to use the technology and how the ISP itself uses the technology. If a system were to force an end-user to share content in exchange for receiving a right to stream or download content, this could lead to an increased sharing of unauthorised content by service users. This in return would incriminate the ISP, because it subjects service users to conditions that necessitate the violation of copyright. Also, if an ISP incentivized file sharing with a loyalty programme it could incriminate itself, should service users share unauthorised content. The ISP could be accused of encouraging end-users to infringe copyright laws.

### 3.3. LEGITIMACY OF nPVR SERVICES

A Network Personal Video Recorder (nPVR) constitutes video recording functionality over the Internet and a remote storage space located on a server of the service provider.\(^{520}\) In effect, the nPVR is a hosted DVR the technological solutions of which are based on cloud computing. Typically, consumers use nPVR services to substitute home VCRs and DVRs, which enable the recording of TV programmes for private use. The consumer controls her nPVR remotely from her television set, computer, or mobile phone that has an access to the Internet.

nPVR service providers commonly generate income from subscription fees collected from service users.\(^{521}\) In Finland, a typical nPVR service provider is a telecom and

---

\(^{520}\) Cf. Copyright Commission (2012); Wikipedia (2013)

\(^{521}\) Copyright Commission (2012), p. 75
Internet operator. They offer nPVR services as by-products alongside a broadband connection and an IPTV service.\textsuperscript{522}

NPVR service providers and broadcasters disagree on the legality of nPVR services. Broadcasters argue that nPVR service providers need licenses\textsuperscript{523} while nPVR service providers plead on the legality of the services on the grounds of private copying exception.\textsuperscript{524}

In theory, two alternate technologies are possible to implement an nPVR service. In the first system, the service provider records programmes on its servers to a “general directory” from which service users stream or download the files on-demand. This model is most likely to be deemed illegal if the service provider has not acquired licenses to reproduce and re-transmit the content. Direct copyright liability emerges on two grounds: firstly, when the service provider unlawfully copies the programmes on its servers, and secondly, when it transmits the programmes to end-users.

Another solution is to reserve a dedicated hard drive space for each client. This model could fall under the private copying exemption, as it would be the user who records the programmes on the server space that she rents. She is also the initiator of the playback; she sends a command to the nPVR system to stream the programme for her.

In its 2012 report, Copyright Commission of the Ministry of Education and Culture of Finland notes that in evaluating the legitimacy of nPVR services under the private copying exemption five interrelated factors should be examined.

1. Has the nPVR service provider acquired the programmes that service users record on the servers lawfully?\textsuperscript{525}
2. Who makes the copy? Even though the request to record a programme reminds the functioning of a home VCR or DVR from the consumer perspective, technically it is the service provider who makes the copy.\textsuperscript{526}
3. For which purpose is the copy made?\textsuperscript{527}
4. What happens to the copy after it is made?\textsuperscript{528}
5. Does the service provider receive commercial advantage or financial gain?\textsuperscript{529}

\textsuperscript{522} Copyright Commission (2012), p. 75
\textsuperscript{523} Cf. MTV3 (2013) and Copyright Commission (2012)
\textsuperscript{524} Cf. Laitila (2012)
\textsuperscript{525} In Finnish: “laillisen lähteen vaatimus”. Cf. Copyright Commission (2012), p. 87
\textsuperscript{526} Cf. Copyright Commission (2012), p. 87
\textsuperscript{527} Id.
\textsuperscript{528} Id.
3.3.1. United States and Australia

One of the first lawsuits in the field of nPVR technologies was Cartoon Network v. CSC Holdings (hereafter ‘Cablevision’)\(^{530}\) in the United States. In 2006, Cablevision launched a remote storage digital video recording system (‘RS-DVR’), which combined functionality of traditional home DVR with video-on-demand (VOD) services.\(^{531}\)

Cartoon Network asked the Court of Appeals to rule that Cablevision was liable for direct copyright infringement on the grounds of making unauthorised reproductions and engaging in unauthorised public performances of Cartoon Network’s works.\(^{532}\) Cablevision had licensing agreements with Cartoon Network, which allowed it to re-distribute Cartoon Network’s programmes on its cable television network.\(^{533}\) However, the licenses did not cover the new RS-DVR streaming technology on the Internet.

In order to be able to re-transmit the programmes of Cartoon Network via the RS-DVR system Cablevision divided the data stream it received from Cartoon Network into two: one data stream went to the cable network and another was directed to a Broadband Media Router (‘BMR’).\(^{534}\) The tasks of the BMR are to buffer and reformat the data and forward it to a server.\(^{535}\) The splitting of the original data stream, the buffering of the data and the storing of the data on the server occur before a customer has made a request to record any of the programmes.\(^{536}\) In the server, programmes are transmitted into the “primary ingest buffer” at which point the server automatically inquires if any customer wants to record programmes.\(^{537}\) If a customer requests a particular programme the request data is transmitted from the primary buffer into a secondary

---

\(^{529}\) Copyright Commission (2012), p. 87  
\(^{530}\) Cartoon Network LP, LLLP v. CSC Holdings, Inc., 536 F.3d 121 (2d Cir. 2008)  
\(^{531}\) Id. p. 1  
\(^{532}\) Id. p. 1, 2  
\(^{533}\) Id. p. 2  
\(^{534}\) Id.  
\(^{535}\) Id.  
\(^{536}\) Id. p. 4  
\(^{537}\) Id. p. 2
buffer, and finally to a space on a hard disk allocated to that customer.\textsuperscript{538} All buffers store programmes only temporarily for 0.1 – 1.2 seconds.\textsuperscript{539}

\textit{Cartoon Network} claimed that \textit{Cablevision} directly infringed their copyright in three ways: (1) by storing (copying) data in the buffers of the system, (2) by storing (copying) playback copies of programmes onto its server, and (3) by transmitting the playback copies to customers.\textsuperscript{540} In reference to the first claim the Court of Appeals opined that programmes are “embodied” in the buffers only for a transitory duration, which does not constitute a fixation of works.\textsuperscript{541} Consequently no copying occurs in the meaning of the Copyright Act and hence \textit{Cablevision} does not violate \textit{Cartoon Network’s} exclusive reproduction right.\textsuperscript{542} In terms of the second claim, the Court chose to interpret that within the RS-DVR system customers create the copies of programmes and that the role of \textit{Cablevision} is to provide the system for reproduction, which in itself does not constitute direct copyright infringement.\textsuperscript{543} In relation to the third claim, the Court stated that the transmission of programmes to customers does not constitute a transmission to the public, because the transmission is directed only to a single subscriber using a single unique copy produced by the subscriber herself.\textsuperscript{544} Consequently, \textit{Cablevision} does not infringe \textit{Cartoon Network’s} exclusive right of public performance.\textsuperscript{545}

In spring 2013, the same Court of Appeals came to similar conclusions in \textit{WNET v. AEREO}.\textsuperscript{546} \textit{Aereo} is a television programming service on the Internet with a remote DVR.\textsuperscript{547} It enables subscribers to watch television with a 10-second delay compared to the original transmission\textsuperscript{548} on the terrestrial television network. Subscribers pay a monthly fee.\textsuperscript{549} Currently, \textit{Aereo} airs programmes only in the New York City.\textsuperscript{550} It has not acquired licenses from broadcasters to record or transmit their programmes.\textsuperscript{551}

\begin{itemize}
\item \textsuperscript{538} Cartoon Network LP, LLLP v. CSC Holdings, Inc., 536 F.3d 121 (2d Cir. 2008), p. 2
\item \textsuperscript{539} Id.
\item \textsuperscript{540} Id. p. 3
\item \textsuperscript{541} Id. p. 7
\item \textsuperscript{542} Id.
\item \textsuperscript{543} Id. p. 11
\item \textsuperscript{544} Id. p. 16
\item \textsuperscript{545} Id. p. 16
\item \textsuperscript{546} WNET et al. v. AEREO Inc., 106 U.S.P.Q.2d 1341 (2nd Cir. 2013)
\item \textsuperscript{547} Id. p. 6
\item \textsuperscript{548} Id. p. 5, 6
\item \textsuperscript{549} Id. p. 5
\item \textsuperscript{550} Id.
\item \textsuperscript{551} Id. p. 6
\end{itemize}
The subscriber can choose to access Aereo’s service with any device with an Internet connection. She can select to watch a programme live or to record it. She can also pause the live programme and rewind it backwards up to the point when she started watching the programme. If she decides to record a programme, from her point of view, this follows the logic of a traditional DVR.

The backend of the Aereo system comprises large antenna boards at its facility in Brooklyn. Each board contains approximately eighty small antennas which each receives broadcast television via the terrestrial network.

"When an Aereo user selects a program to watch or record, a signal is sent to Aereo’s antenna server. The antenna server assigns one of the individual antennas and a transcoder to the user. The antenna server tunes that antenna to the broadcast frequency of the channel showing the program the user wishes to watch or record. The server transcodes the data received by this antenna, buffers it, and sends it to another Aereo server, where a copy of the program is saved to a large hard drive in a directory reserved for that Aereo user. If the user has chosen to "Record" the program, the Aereo system will create a complete copy of the program for that user to watch later. When the user chooses to view that program, Aereo's servers will stream the program to the user from the copy of the program saved in the user's directory on the Aereo server. If the user instead has chosen to “Watch” the program, the same operations occur, except that once six or seven seconds of programming have been saved in the hard drive copy of the program in the user's directory on the Aereo server, the Aereo system begins streaming the program to the user from this copy."556

Various broadcasting companies including WNET asked the Court of Appeals to rule that Aereo’s transmission of their television programmes infringed their exclusive right to publicly perform their works. The Court relied heavily on the Cablevision decision finding that Aereo makes multiple private transmissions of the same work, which cannot be considered as a public performance. The broadcasters filed a petition with the Supreme Court in October 2013. They argue that Aereo is “stealing their broadcast signal” which should be deemed illegal. They receive support from Professor Jane Ginsburg who criticises the Cablevision and Aereo rulings, because they undermine the

553 Id. p. 6
554 Id. p. 6-7
555 Id. p. 7
556 Id. p. 9
557 Id. p. 5
558 Id. p. 26, 35
559 Fixmer (2013)
public performance right of broadcasters allowing new business models of digital content delivery to evade copyright liability.560

Also in Australia, Judge Rares of the Federal Court decided in February 2012 in **Optus v. National Rugby League**561 that the nPVR service “TV Now” of Optus did not infringe the reproduction or communication right of rights holders.562 The reasoning of the Court was identical with the Court of Appeals of the 2nd Circuit in **Cablevision** and **Aereo**. The Court stated that it is the user of the service who produces the copy in a similar manner as if she were using a VCR or DVR.563 Further, despite the fact that Optus “provided all the significant technology for making, keeping, and playing the recording, this was no different to a person using equipment or technology in his or her home or elsewhere to copy or record a broadcast”.564

Two months later the Full Federal Court reversed Judge Rares’ decision and found Optus liable for direct copyright infringement.565 The Court argued that either Optus alone or Optus and subscribers jointly made copies of programmes.566 It reasoned that “[w]ithout the subscriber’s involvement, nothing would be created; without Optus’ involvement nothing would be copied.”567 The Court also considered it as a relevant factor that Optus made copies of programmes for subscribers in order to derive market advantage in the digital TV industry.568 In its conclusion, the Court noted that in the most important question of “who makes the copy” the answer depends on two factors: the relationship between the service provider and subscriber as well as the characteristics of the technological solutions used to carry out the service.569 The Court did not address the question of distributing the works to the public.

---

560 Ginsburg (2013)
561 Singtel Optus Pty Ltd v. National Rugby League Investments Pty Ltd (No 2) [2012]
562 Id. p. 4
563 Id.
564 Id.
565 National Rugby League Investments Pty Ltd v. Singtel Optus Pty Ltd [2012], FCAFC 59 at 93
566 Id. at 79
567 Id. at 76
568 Id. at 89
569 Id. at 100
3.3.2. Europe

In Germany, three nPVR cases were argued before the Supreme Court of Germany (Bundesgerichtshof) on the same day in 2009. Two major broadcasters RTL and SAT1 had brought actions against Shift.TV and Save.TV in 2006 and 2007. Both nPVR service providers captured the television signals of RTL and SAT1 via satellite and retransmitted the programmes to their clients. Each client had a dedicated storage space on the servers of the service providers. The Court concluded that nPVR service providers are likely to infringe broadcasters’ copyrights depending on the technical solutions they use to carry out the service.

The Supreme Court first considered the question of who performs the reproduction in nPVR systems. The Court held that the person performing the reproduction is the person who technically triggers the copying. Thus, if an nPVR service is structured so that customers always trigger the copying, the service provider does not perform the reproduction of works. If service users make copies for private purposes, they can rely on the statutory private copying exemption. In this scenario, the service provider would not infringe the rights holders’ right of reproduction.

The Court noted that a service provider becomes liable for copyright infringement if it performs the act of copying, unless it makes only single copies for a customer free of charge. This means that the private copying exception applies only to single copies made for private purposes by the customer herself or by a non-profit organisation.

In the question of whether nPVR service providers make works available to the public, the Court opined that service providers do not infringe the exclusive right of copyright holders if they allow a service user to access the copy intended for her exclusive use.

---

570 Niemann (2009)
571 ProSievenSat.1. v. Shift.TV, Az. I ZR 215/06, April 22, 2009 and RTL v. Shift.TV, Az. I ZR 216/06
572 RTL v. Save.TV, Az. I ZR 175/07, April 22, 2009
573 Niemann (2009)
574 Id.
575 Id.
576 Id.
577 Id.
578 Id.
579 Id.
580 Id.
581 Id.
582 Id.
even if the service providers offered identical copies of the same programme to multiple persons.\textsuperscript{583} However, an unauthorised retransmission occurs when a customer watches (“performs the retransmission”) the programme.\textsuperscript{584} Broadcasters’ right to make works available to the public is infringed if a service provider retransmits a broadcasting signal simultaneously to a sufficient number of customers, as this forms a “public”.\textsuperscript{585}

The Supreme Court referred the consolidated cases back to the Higher Regional Court of Dresden, which in 2012 came to the conclusion that nPVR service providers had infringed the exclusive rights of broadcasters in terms of making works available to the public without permission.\textsuperscript{586} The conclusion was based on a finding of RTL and SAT1 that succeeded in proving that a transmission had taken place when TV signals related to a single programme had been transmitted to at least ten different recipients simultaneously.\textsuperscript{587} The Court further stated that the nPVR service providers did not infringe the reproduction right of broadcasters. The Court considered the service user to be the reproducer, in which context the nPVR was only an auxiliary device, which supported the end-user in the production of private copies.\textsuperscript{588}

Shift.TV and Save.TV appealed to the Supreme Court, which in spring 2013 confirmed that nPVR services need licenses\textsuperscript{589} from broadcasters to re-transmit their television signals.\textsuperscript{590} On the basis of this ruling, streaming recorded programmes to nPVR clients constitutes a transmission of works to the public. This means that nPVR service providers are subjected to the same treatment as cable television service providers.\textsuperscript{591}

In Finland, the District Court of Helsinki heard its first nPVR case, TVkaista, in November 2013.\textsuperscript{592} It is likely that TVkaista will not make a perfect precedent concerning the legitimacy of nPVR services in Finland, because the evidence suggests that the owners of the service have committed a fraud.\textsuperscript{593} In 2009, the police found a fake server room on the premises of TVkaista with 2,996 recorders that were not

\textsuperscript{583} Niemann (2009)  
\textsuperscript{584} Cf. id.  
\textsuperscript{585} Id.  
\textsuperscript{586} Lovells et al. (2012)  
\textsuperscript{587} Id.  
\textsuperscript{588} Id.  
\textsuperscript{589} Pachali (2013)  
\textsuperscript{590} See: Sa-1 ve.TV v. RTL Az. I ZR 151/11, April 1, 2013; Shift.TV v. RTL, Az. I ZR 152/11, April 1, 2013; and Shift.TV v. Sat.1, Az. I ZR 153/11, April 1, 2013.  
\textsuperscript{591} Pachali (2013)  
\textsuperscript{592} Laitila (2013)  
\textsuperscript{593} Id.
connected to the electrical grid or data network.\textsuperscript{594} Hence, it seems that \textit{TVkaista} stored copies of programmes on “general directories” from which it streamed the programmes to customers at their request.\textsuperscript{595} This will most likely incriminate \textit{TVkaista}’s owners. Finnish broadcasting organisations are planning additional legal actions against telecom operators Elisa and TeliaSonera for their respective nPVR services.\textsuperscript{596}

\section*{3.3.3. Conclusions}

NPVR technologies are new. This shows in the work of international courts which have been struggling to define who reproduces programmes, whether making works available to the public occurs, and which parts of the services constitute private copying. German and Australian courts agree that the definition of who makes the copy depends on the technical solution of the nPVR system. At the time of writing this thesis, the legality of nPVR technologies has been evaluated as follows:

- In the United States, the end-user makes the copy. Hence, no copyright infringement takes place on the part of the nPVR service provider when television programmes are reproduced on its servers. There is no public performance of a work either, because the work is distributed to a single person at a time. A public performance can occur only if there is a public. NPVR service providers do not infringe broadcasters’ public performance right.

- In Australia, the service provider alone or the service provider and the service user jointly make the copy depending on the technological solution. Either way, nPVR service providers violate directly rights holders’ reproduction right. A legal uncertainty exists in regard to whether a public transmission takes place.

- In Germany, the end-user makes the copy. No copyright infringement occurs, as this falls under the private copying exception. The re-transmission of programmes constitutes making programmes available to the public. For this nPVR service providers need licenses from broadcasters.

\textsuperscript{594} Laitila (2013), Vänskä (2013)
\textsuperscript{595} Cf. id.
\textsuperscript{596} M&M (2012), Laitila (2012)
4 VIABLE E-BUSINESS MODELS FOR MEDIA ISPS

The objectives of this study have been to find out what kinds of e-services are legitimate in the content industries and what kinds of e-business models are viable for media Internet service providers (ISPs). The legality of e-businesses has been examined by studying copyright disputes in which the legitimacy of services and service technologies of news aggregators, file hosting service providers and NPVR service providers has been questioned. The aim of this chapter is to summarise and generalise the research findings from the case analyses.

The findings suggest that media ISPs have an increased risk of infringing copyright laws. Primarily, copyright liability for a media ISP emerges when service users communicate unauthorised content to the public and the ISP fails to remove the infringing content or hyperlinks and URLs leading to that content. ISP liability can also result from the facilitation of content and data exchange between service users if the exchanged content is used without permission. Also, the use of hyperlinks and URLs to third party websites can trigger copyright liability if an ISP has not obtained permission to link third party content to its website.

When dealing with copyrighted works or hyperlinks, the only way to achieve certainty of not becoming liable for a copyright infringement is to have solid licensing agreements with rights holders. If it is not feasible or possible to acquire licenses, an ISP can reduce the risks of becoming a target for copyright lawsuits by exercising good judgement and being circumspect. The following sections discuss factors that a media entrepreneur should take into consideration when planning an online media service. A media ISP should have a plan for how the exploitation rights to content are acquired, what the service users are allowed to do on the website, how the content monitoring and takedown procedures are carried out, and what the linking policy is.
An essential part in the development of a media e-business model is to decide how the ISP acquires content for the service. There basically are three alternatives: the service provider itself creates the content, the service provider asks service users to create the content, or the service provider re-uses existing works with or without licenses.

Indeed, the service provider can produce the content itself. We call this the self-production model. To be able to use the content in commerce, the service provider has to acquire permissions from the employees and suppliers who create the content. The permission can be acquired as an assignment (transfer of ownership of works) or as a license (transfer of exploitation rights) in employment agreements or in separate contracts. ISPs that apply the self-production model operate in the same manner as traditional publishing companies. The ISP is liable for the published content. It has to apply journalists’ codes of ethics including pre-emptive self-regulation.

The service provider can also acquire content from film studios, record labels, broadcasting companies, publishing houses, and other rights holders with prominent back catalogues. A prerequisite for the success of this content acquisition model is that the service provider is able to negotiate reasonable licensing agreements with the rights holders. This model can be referred to as the licensing model. For instance, Netflix, HBO Nordic, iTunes, and Spotify use this model to build their libraries.

In the licensing model, a bottleneck for media ISPs could be the so-called access fees imposed by multi-national media conglomerates. Access fee refers to payments related to acquiring access to a rights holder’s content catalogue. For instance, Spotify is rumoured to have unsatisfactory licensing agreements with major record labels. “The majors know that no one can start a viable digital music platform without their content and as a result they use their considerable power to shape the digital landscape and influence the business practices of streaming services.” The licensing agreements are assumed to be a reason for why it will be difficult for Spotify to become profitable, as the costs of building the content library are likely to exceed the

---

597 Cf. Lindvall (2013)
598 Id. (2013)
600 Nick O’Byrne, General Manager of the Australian Independent Record Labels Association, in Fitzsimons (2013)
For this reason, online media service providers might want to resort to alternate content acquisition models.

An alternative could be a **UGC model** ('user-generated content' model) in which the service provider uses crowdsourcing by asking service users to produce the content. In the UGC model, the service provider needs to acquire the permission to distribute the content from service users who are the creators of the content. The permission is acquired as a part of the user agreement. Typically, social networking sites and content sharing services such as Facebook, Twitter, YouTube, Flickr, and Pinterest use this model. The problem related to these services is that also proprietary content circulates in their systems, because it is impossible to police the behaviour of each service user pre-emptively. As a consequence, service providers that aim at a UGC model usually end up deploying a hybrid model in practice.

The **hybrid model** is a combination of the licensing and UGC models. ISP safe harbour laws, and often also business agreements, require that firms which use the UGC or hybrid model deploy content filtering solutions to remove unauthorised content. Often the business agreements also require that the ISP compensates the rights holders by paying a share of its advertising and data aggregation revenue or subscription fees.

Yet another alternative could be to require that content creators who use the service waive their right to enforce their copyrights for those parts that the rights can be waived. Rights holders can waive all their economic rights apart from compulsory licenses imposed by the state. This model could be referred to as the **copyleft model**. In this model, the ISP deploys Creative Commons or Open Source licenses to avoid copyright liability. Examples of online services in which many service users license their works under the Creative Commons are the image and video sharing service Flickr and the photo sharing service Picasa. Also, the Qatari television network Al Jazeera publishes posts by prominent journalists under a Creative Commons license.

A firm could also take a risk and try to deploy copyright limitations, fair use principles or ISP liability limitations to avoid copyright liability. It can also utilise works in the

---

601 Cf. Robertson (2011)
602 Creative Commons (n.d. a)
603 Id.
604 Cf. Gietke (2012)
public domain. We call this the *copyright-avoiding model*. Service providers that currently could be perceived to test the possible loopholes of copyright laws are NPVR service providers. Also, some cyberlockers could fit the description.

All the above-mentioned content acquisition models, apart from the copyright-avoiding business model, presuppose a transfer or a waiver of copyrights. The “copyleft model” deploys existing Creative Commons and Open Source licenses. In terms of voluntary copyright licenses, distribution licenses between media ISPs and rights holders are most common. They allow an ISP or its service users to make content available within the service. Reproduction licences are needed if service users are allowed to download or upload content or if the ISP itself stores proprietary content on its servers. A need for adaptation licenses would emerge if service users were allowed to make derivative works, i.e. to remix, appropriate or mash up content, or if the service provider itself wanted to make changes (e.g. shorten or summarise) to existing works.

In a copyright licensing agreement, the following matters should be clearly stated:

- **Economic rights**
  - Which rights (reproduction, distribution, adaptation) are licensed?
  - For what purposes can work(s) be exploited?
  - In which territories can work(s) be exploited?
  - Is the license exclusive or non-exclusive?
  - What is the duration of the license?
  - How much does the licence cost? Does the compensation constitute a one-off payment, royalties from streaming/downloads, or a share of revenue?

- **Moral rights**
  - How is the author to be attributed when her work(s) are distributed?
  - Does the author waive her right of being identified as the author?
  - Does the author want to limit the adaptation or distribution of her works in some way?

---

605 Cf. id.
4.2. WHAT ARE SERVICE USERS ALLOWED TO DO?

When designing the functionality of an online service, the service provider defines what kinds of operations service users are allowed to perform. For instance, an online television service provider would need to make a decision at least in terms of whether the service is carried out as a simulcast or an on-demand service. In addition, the service provider would need to decide whether the service users were allowed to download, upload and share content within the service.

In a simulcast, the viewer can watch a television programme on the Internet simultaneously as it is broadcasted on the television network. Many television and film service providers also offer video on-demand (VOD) services. VOD is based on the principle that the customer can access the content when it is convenient for her. In a VOD system, the service provider stores television programmes on its servers from which the service users can stream (‘playback’) the recordings. In a user agreement, the permission to stream a recording could be referred to as a “license to play”.\textsuperscript{606} The service provider could also grant service users a permission to download programmes on their computers. This could be called a “license to copy”.\textsuperscript{607}

If service users are only allowed to play (stream) the content, the service provider has to acquire reproduction and distribution licenses for itself from the rights holders. It also has to deploy technical protection measures (TPMs) to prevent the service users from copying the programmes it hosts. If service users are also permitted to download content, the service provider needs to acquire a distribution license for itself and reproduction licenses for itself and the service users. The rights holders can also require that their programmes be embedded with TPMs to restrict the amount of copies that the service users can reproduce from the programmes. The user agreement should also include a clause that prohibits the communication and distribution of the programmes to the public. If the service provider allows the service users to play, copy and share programmes, it has to acquire reproduction and distribution licenses for itself and the service users. Embedding TPMs in media files that can be shared indefinitely would not be an option.

\textsuperscript{606} Cf. Günther (2010), p. 2
\textsuperscript{607} Cf. id.
It is noteworthy that technically copying occurs also when media files are streamed. The functioning of the Internet requires *caching*. Caching is needed to ensure speedier access to websites for Internet users.\(^{608}\) This means that temporary copies of files that are being transferred on the Internet are commonly reproduced in the proxy servers of ISPs. ISPs are protected from copyright liability with ISP safe harbour statutes.\(^{609}\)

When a service user watches a video on a streaming service, her computer also copies excess data in a buffer.\(^{610}\) This constitutes a reproduction of a work in part, which falls under the exclusive rights of rights holders. Individuals are permitted to make temporary copies on the basis of copyright limitations. For instance, Section 11a of the Copyright Act 404/1961 of Finland permits temporary reproduction, with the exception of computer programmes and databases, if the reproduction is (1) transient or incidental, (2) integral and essential part of a technological process, and if (3) its sole purpose is to enable a transmission of a work in a network between third parties by an intermediary or a lawful use of a work, and if the reproduction (4) has no independent economic significance.

Also, uploading constitutes copying. When a service user uploads content in order to store or share it, a copy of the work is stored on the service provider’s server. When a copy is stored for the purpose of preserving the work for future deployment, the ISP becomes a file hosting service and it loses its safe harbour as a provider of caching functionality. If the stored file contained unauthorised content, the service provider could risk being accused of copyright infringement. In order to avoid copyright liability it has to qualify for the ISP safe harbour created for hosting services. There is only one way for a file hosting service provider to become eligible. The ISP has to succumb to the notice-and-takedown procedure. Consequently, the ISP should devise its user agreements and terms of service in a manner that allows it to remove UGC without further legal actions on the part of service users. The terms should however be as fair as possible. A high-handed treatment of service users would be bad service, the consequences of which could lead to a loss of service users.

The question of whether the uploading of content can constitute copyright infringement depends on the lawfulness of the content. There is no problem if the service user is the rights owner. It is a different matter when a service user uploads proprietary content on

---

\(^{608}\) Samuelson (2006), p. 142

\(^{609}\) For instance, safe harbours for ISPs are stated in Articles 12-15 of the E-Commerce Directive of the EU and in §512 of 17 USC in the United States.

\(^{610}\) Webopedia (2013c)
the servers of the ISP without authorisation. This would expose the ISP for indirect liability charges. If the service user merely uploaded proprietary content in order to store a backup copy without intent to distribute it, would this constitute copyright infringement? The answer depends on whether the copying constitutes private reproduction.

International copyright legislation permits private copying with certain limitations. In Finland, Copyright Act 404/1961, §12 allows the reproduction for private use on the following grounds:

[1] Anyone may make single copies for his private use of a work that has been made public. The copies thus made may not be used for other purposes.

[2] It is also permitted to have copies made by a third party for the private use of the party ordering the copies.

[3] The provisions of subsection 2 shall not apply to the reproduction of musical works, cinematographic works, utility articles or sculptures, or the reproduction of any other work of art by artistic means.

[4] The provisions of this section shall not apply to a computer-readable computer program, to the making of a computer-readable copy of a computer-readable database, or to the construction of a work of architecture.

The first question here is whether the uploading of copyrighted works on a remote server of an ISP can be interpreted as private reproduction when the service user initiates the uploading. If it does not constitute private reproduction, the uploading would make the service user a direct infringer and the service provider indirect infringer. Another question is whether the uploading could be interpreted as “having copies made by a third party” in the meaning of §12[2]? After all, it is the service provider that provides the copying technology and the storage facility. If copying was interpreted as “copies made by the service provider” would this mean that on the basis of §12[3] the uploading of music, films, and television programmes would constitute copyright infringement, while the uploading of literary works would be allowed? The law is not clear in this respect. Copyright laws are currently being tested by cloud storage and nPVR services.

Permitting service users to only access or stream content is the safest alternative for ISPs. If service users are allowed to download, upload and share content, the risks for
copyright violations increase. The ISP can reduce the risks to some extent if it requires service users to register for the service. The service users that have registered with their own names are likely to commit less copyright violations. However, the registering does not create a waterproof system, as there are always individuals who fabricate their identities or who are ignorant of copyright. Nevertheless, the requirement to register could be a mitigating factor should an ISP end up in court. An ISP can also limit copyright liability by abstaining from offering rewards to service users who download, upload, or share content, as a court could interpret this as an encouragement to commit copyright infringements if unauthorised content was circulated.

4.3. CONTENT MONITORING AND TAKEDOWN

Media ISPs seldom qualify for the safe harbours created for ISPs operating as “mere conduits.” The “mere conduit” exemption is mostly available for telecom and Internet operators that merely provide access services to communications networks. But even they cannot afford to turn a blind eye to copyright violations. The law obligates a “mere conduit” to terminate or prevent an infringement if it receives an order from a court. Several court orders have recently required telecom operators to block access to infringing websites and to actively police domains that provide access to services that are known to distribute unauthorised content.611 Especially, the BitTorrent service The Pirate Bay has proven to be difficult to shut down.

A typical ISP hosts media files. It may be exempt from copyright liability if it succumbs to the notice-and-takedown procedure stated in Article 14(1)(b) of the E-Commerce Directive. At the time of writing of this thesis, there are no judicial requirements in the EU for how a notice of an alleged copyright infringement should be given and how an ISP should respond to the notice. However, there is an obligation that a hosting service provider cannot escape: An ISP is obligated to expeditiously remove or disable access to infringing content upon obtaining knowledge of specific infringing files. Failing to fulfil this duty is likely to make it liable for indirect copyright infringement. In addition, several court orders have required a file hosting service provider to start using content

monitoring and filtering software to detect and remove infringing files residing on its servers. This may require significant monetary investments from the ISP.

Content filtering can be carried out in two ways: manually and automatically. In practice, most file hosting service providers use both. The current automated and human-induced takedown practices have been widely criticised. First of all, the automated filtering systems produce erroneous takedown notices. ISPs need to have policies for how to deal with service users whose content or account has been removed by mistake. Secondly, a removal can occur based only on a single complaint, the legitimacy of which is not necessarily investigated before executing the corrective measures. Thirdly, rights holders have been accused of abusing the notice-and-takedown procedure to censor criticism and to hamper the business activities of competitors. On some occasions, a rights holder has overstated its claims in order to eliminate possible future threats or to hamper the business of an ISP that it accuses of hosting illegal content. Because of the judicial requirement to act without delay, an ISP usually does not have time to investigate the legitimacy of a takedown notice. It rather takes the risk of making one service user angry than facing a multinational conglomerate with limitless monetary resources in court.

Despite the fact that the service user is usually allowed to dispute the takedown or the suspension of her account with a counter-notice, before the law and on the basis of user agreements, service providers have the possibility to ignore the counter-notice without legal consequences. This is bad service and an opportunity for a service-oriented media ISP to attract service users from its competitors.

The legal risks involved in hosting UGC necessitates that a media ISP has a workable policy for how to monitor and remove content and how to inform service users if they are suspected of copyright infringements, or if their content or account is removed. Also, increasing the transparency of how the monitoring is conducted and whether the monitoring can lead to a disclosure of personal data would help to build trust between the service provider and the service user. A workable reclamation policy could also allow the ISP to gain competitive advantage.

---

612 Holmes (2013), Schruers (2013)
613 Cf. the suspension of the Twitter account of Guy Adams. See more: Shapiro (2012) and Adams (2012).
614 Schruers (2013)
615 Cf. Lee (2011)
616 Gibson (2011)
4.4. HOW TO LINK SAFELY?

The research findings of this thesis suggest that also hyperlinking and framing can result in copyright infringements. In order to reduce legal risks an ISP can take several precautions.

The safest is to seek permission from rights holders especially when using deep links, inlining or framing.\textsuperscript{617} The permission should take the form of a written agreement. If it is not feasible or possible to seek permission, the ISP can place a disclaimer on the web pages on which links and framed content are displayed. In the disclaimer, the ISP should deny any endorsements for or from other websites and authors.\textsuperscript{618} Also, a waiver of liability for accidental distribution or reproduction of unauthorised content could act as a mitigating factor in court if a link or framed content were found to direct the website users to infringing content.\textsuperscript{619}

In the creation of hyperlinks, an ISP can limit legal risks by using insubstantial parts of works both in the link itself and in the possible accompanying description if only feasible. For instance, if you embed a link to a newspaper article, the headline of which is "Prime Minister Found Guilty of Taking Bribes," you should try to avoid all the keywords 'prime minister', 'guilty', and 'bribes'. Instead, you could create a link with characters or words that create a vacuous whole. This practice might not be feasible for news aggregators and search engines, as the information value of their indices would degrade, but for other ISPs this practice could be conceivable.

\textsuperscript{617} Fitzpatrick (2013)
\textsuperscript{618} Cf. id.
\textsuperscript{619} Cf. id.
5 JUDICIAL CONSIDERATIONS

The laws that limit the liability of ISPs do more than they insinuate. The promised safe harbours come with a price. In order to qualify for a safe harbour an ISP can be obligated to remove content, block access to content, and disclose information about service users who are suspected of illegal activities.

Article 15 of the Directive 2000/31/EC states that ISPs cannot be obligated to actively seek facts or circumstances that would reveal illegal activities. This exemption is further demarcated in the Preamble of the Directive. Clause 47 of the Preamble delineates that the provision "No General Obligation to Monitor" concerns obligations of a general nature and that monitoring can be required in specific cases. Thus, the interpretation of Article 15 depends on what is meant with "general nature" and "specific case".

The case analyses of this thesis reveal that courts have issued injunctions that require file hosting service providers to apply keyword filtering to identify and remove content. Some courts have interpreted that when an ISP receives information from a rights holder about specific works that allegedly infringe copyrights, this could be interpreted to constitute a specific case. Can the monitoring of several specific cases become a monitoring obligation of a general nature?

Some rights holders have been accused of overstating and fabricating their takedown requests.\(^{620}\) If dozens or hundreds of rights holders were to supply an ISP with cease-and-desist requests, and if each request would identify dozens or hundreds of works that allegedly are in breach of copyright, wouldn't that gradually accumulate to compose a monitoring system of a general nature? Further, if a significant number of takedown requests were bogus, and legitimate content was removed, wouldn't this frustrate the takedown system as arbitrary?

The current notice-and-takedown practices and content filtering technologies require substantial investments from ISPs. The technological development of content monitoring systems is still at its early stage. Continuous investments are necessary to remediate the technological vulnerabilities. Meanwhile ISPs are required to hire staff to take care of the manual labour of correcting mistakes that automated filtering systems

\(^{620}\) Cf. Schruers (2013), Lee (2011)
cause. Looking after the interests of copyright holders induce costs for ISPs. A well-balanced copyright system would require rights holders to reimburse legitimate ISPs for policing their interests for them. A well-balanced system would also penalise inappropriate uses of takedown notices.

This study has also brought forward the difficulties of demarcating what constitutes private reproduction and public communication in the age of the Internet. Particularly, cloud technologies challenge our understanding of when a person is engaged in private reproduction. The question of whether a remote virtual storage space can be reckoned as an extension of a private space or a home circle has bewildered courts. The current understanding seems to be that a private space can be extended to include virtual spaces on remote servers. However, an uncertainty exists in which circumstances a retrieval of content stored on a cloud constitutes communication to the public. An inclusion of a new limitation to exclusive rights, namely “private communication”, could prove to be a welcomed update in the effort of modernising copyright.

To build a viable and profitable e-business can be a challenge to media entrepreneurs. The acquisition of licenses from rights holders can turn out to be costly. Rights holders can also refuse to license. In the absence of global extended collective licenses (ECLs) and industry-wide standard licensing rates ISPs can be forced to consent to unreasonable contract terms. Without licenses the entrepreneur would risk becoming a target for lawsuits. Losing a lawsuit could result in significant monetary damages and a business closure. In order to promote the legal uses of copyrighted works, a customised version of FRAND (fair, reasonable, and non-discriminatory) licensing used in connection to standard essential patents (SEPs) could be introduced to copyright.

Copyright has its roots in an age when cultural products were distributed as physical copies and the copying and distribution required substantial investments. Only individuals and commercial actors with considerable material resources could reproduce high-quality copies of works and make them available on the market. Today, almost anyone can reproduce a high-quality copy and distribute it to millions of people with extremely low costs. Private citizens have taken possession of the territory that earlier was reserved exclusively for media publishers. This has disrupted the value creation logic in the content industries for good.

Copyright creates artificial scarcity. It is inherent to the copyright system that it incentivises the creation of new works and restricts access to those works. It also
depreciates the value of derivative works, as if stating that “new works” are more deserving to be protected than the productions of the crowd mind, which subjects works to re-thought and revisions. This logic is contrary to what digital and Internet technologies represent. They promote the free circulation and re-use of knowledge and cultural products. Collisions are inevitable. Yet, history has shown that time and market forces tend to provide equilibrium in balancing interests. In the meantime, ISPs and copyright owners are trying to survive in the gales of creative destruction.

“Without the public demand for entertainment, the electronic equipment industry would not be able to sell its machines to the public. Without the facilities provided by the electronic equipment industry, the entertainment industry could not provide entertainment in the home [...]. Although the two industries are interdependent and flourish to their mutual satisfaction there is one area in which their interests conflict. It is in the interests of the electronic equipment industry to put on the market every facility which is likely to induce customers to purchase new machines made by the industry. It is in the interests of the entertainment industry to maintain a monopoly in the reproduction of entertainment.”

Lord Templeman (1988)
CBS Songs v Amstrad Consumer Electronics

---

621 Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd, 380 F. 3d 1154 (9th Cir. 2004) at 1167
622 CBS Songs Ltd v Amstrad Consumer Electronics Plc. [1988] AC 1013
CORE CONCEPTS

**Author:** The creator of a copyrighted work.

**Business model:** Methods and means of conducting a business with the objective to create value of and capture value from the products and services of the company.

**Cloud service:** An online service allowing a remote storage of data and media files and the distribution of the files over the Internet (see also ‘cyberlocker’).

**Content industries:** Industries in which the exchange of music, literary, artistic, or audio-visual works forms the basis for generating income directly or indirectly.

**Copyright:** A limited legal monopoly right afforded to the creator of a literary or artistic work, or a third party to which the creator has transferred the rights, to reproduce, make available, and adapt the work.

**Cyberlocker:** A file hosting service provider that provides server space for remote file storing accompanied with file-sharing functionality over the Internet.\(^{623}\)

**Electronic business (e-Business):** A commercial practice of producing, distributing, marketing or otherwise communicating products, services and information on the Internet or other communication networks.

**End-user:** A consumer or a company who is assumed to be the last actor in the value chain to use a product or a service.

**File hosting service:** A service in which the service provider stores and possibly allows the distribution of data and media files provided by service users.

**Framing:** A form of linking, where a website operator incorporates third party content in its own web page in a manner that creates an appearance of a unitary whole.

**Hyperlinking:** The distribution of a word, phrase, or image that one can click on to move to a new web page, document, or section within the current document.\(^{624}\)

**Index:** A record of data or a database that uses key words to sort data. Consequently *indexing* is the act of creating a record of data or database.

**Infringement:** A violation of a right, law, or contract.

---

\(^{623}\) Janssen (n.d. a)

\(^{624}\) Cf. TechTerms.com (2013)
**Intermediary service provider:** An individual or company which on a communication network (a) operates as a *merely conduit* providing the means to transmit data, (b) optimises the transmission of data by providing an automatic, intermediate and temporary storage of data in a form of *caching* technology, or (c) *hosts* an automated *data storage and distribution service*.625

**Internet service provider (ISP):** A firm that provides or facilitates the storing and distribution of content and access to content on the Internet. Typically, an ISP is a file hosting website, social networking website, blogging service, news aggregator, search engine, or telecommunications operator.

**Liability:** Legal responsibility for one’s actions or failure to meet a responsibility.626

**Media:** Broadcasting and narrowcasting channels such as television, radio, newspapers, magazines, the Internet, telephone, fax, direct mail, and billboards, which allow the dissemination of news, entertainment, education, data, and promotional material627

**Media content:** Literary, visual, video, audio or music information capable of being distributed by the means of mass communication (mass media) technologies such as newspapers, magazines, books, the Internet, television, radio, and cinema.

**Media ISP:** A firm that facilitates the production, distribution, and storing of user-generated media content or the re-use of extant media content on the Internet.

**Micro-blogging:** The act of publishing short text updates (called micro-posts)628 for instance on social networking sites.

**News aggregator:** An automated website that searches and collates news headlines and news excerpts and publishes them as indices on the Internet.

**nPVR:** An abbreviation of *Network Personal Video Recorder*.629 An nPVR is a video recording function and a storage space on a service provider’s server that a customer controls remotely. An nPVR system can also be referred to as *nDVR* (Network Digital Video Recorder) and *RS-DVR* (Remote Storage Digital Video Recorder)630 or Remote Server Digital Video Recorder.631

**Online:** To be connected to the Internet and Internet users by using an Internet-connectable device such as a computer or mobile phone.

---

625 Cf. EU Directive on Electronic Commerce, Articles 12-14
626 Law.com (n.d.)
627 BusinessDictionary.com (2013b)
628 Webopedia (2013a)
629 Copyright Commission (2011)
630 Wikipedia (2013)
631 Ivdictionary.com (n.d.)
**Rights holder:** The creator of a copyrighted work, an heir, or a third party to whom the creator has licensed or assigned her economic rights.

**Safe harbour:** A statutory or regulatory provision, which provides protection from liability or penalty if certain conditions are met.⁶³²

**Service:** The process of delivering a product, facility, data, information, function, or other utility to the market.

**Service provider:** An individual or a company who provides a service.

**Service user:** An individual or a company who uses a service.

**Social media:** “Websites and applications that enable users to create and share content or to participate in social networking.”⁶³³

**Social networking service:** An online service allowing Internet users to make connections with one another and to form online communities.⁶³⁴

**Telecommunications:** Communication over a distance by using telephones, telegraph, radio, microwave technologies, fibre optics, satellites and the Internet.⁶³⁵

**Telecommunications operator (telecom operator):** A company maintaining and providing access to a communications network utilising telecommunications technologies (see ‘Telecommunications’).

**UGC:** An abbreviation of *User Generated Content*. UGC is media content that is created and published by the users of an online service.⁶³⁶

---

⁶³² BusinessDictionary.com (2013a)
⁶³³ Oxford Dictionaries (2013)
⁶³⁵ Janssen (n.d. b)
⁶³⁶ Webopedia (2013b)
SCIENTIFIC LITERATURE AND WEB ARTICLES


Creative Commons (n.d. a): ”Who uses CC?” Accessed 20.11.2013. Available at: http://creativecommons.org/who-uses-cc

Creative Commons (n.d. b): “About the Licenses”. Creative Commons. Accessed 30.11.2013. Available at: http://creativecommons.org/licenses/


STATUTES, TREATIES, AND CONVENTIONS

Agreement on Trade-Related Aspects of Intellectual Property Rights (1994)

Berne Convention for the Protection of Literary and Artistic Works (1886)

Copyright Act 1968 (of Australia) (amendments up to Act No. 94 of 2010 included)

Copyright Act (Tekijänoikeuslaki) 8.7.1961/404 (amendments up to 674/2013 included). Quotations used from the unofficial English translation (amendments up to 307/2010 included)


The Act of Copyright and Related Rights of Germany. English translation, (amendments up to 17.12.2008 included)

The Act on the Provision of Information Society Services (Laki tietoyhteiskunnan palvelujen tarjoamisesta) 5.6.2002/458 (amendments up to 677/2012)

WIPO Beijing Treaty on Audiovisual Performances (2012)

WIPO Copyright Treaty (1996)

WIPO Performances and Phonograms Treaty (1996)
<table>
<thead>
<tr>
<th>TABLE OF CASES</th>
</tr>
</thead>
</table>


Milorad Trkulja v Google Inc LLC & Anor (No 5) [2012] VSC 533, November 12th 2012, Supreme Court of Victoria, Australia. Accessed 7.11.2013. Available at:


