Master Thesis

Internet Service Provider liability for third-party copyright infringement
A comparative study between US and EU approaches

To what extent should an ISP be held liable for third-party copyright infringement?

Taragade Dangngam   Anr.752235
Thesis supervisor:  Dr. Colette Cuijpers
Law and Technology, Faculty of Law
Tilburg University
August 2009
Table of Content

Chapter 1: Introduction
1.1 Study Background........................................................................................................5
1.2 Research question........................................................................................................8
1.3 Methodology................................................................................................................8
1.4 Structure of thesis........................................................................................................9

Chapter 2: General issues of ISPs liability for copyright infringement
2.1 Introduction................................................................................................................10
2.2 Internet Service Provider...............................................................................................10
2.3 Reason for pursuing claim against Internet Service Provider........................................12
2.4 Type of liability............................................................................................................13
2.5 Area of potential liability.............................................................................................14

3.1 Introduction................................................................................................................16
3.2 Pre-DMCA..................................................................................................................17
   3.2.1 Kind of liability......................................................................................................17
       3.2.1.1 Direct liability...............................................................................................17
       3.2.1.2 Secondary liability.......................................................................................19
           3.2.1.2.1 Vicarious liability................................................................................19
           3.2.1.2.2 Contributory liability............................................................................22
       3.2.2 The Analysis of rules governing ISP liability for third-party copyright infringement
           in the era of Pre-DMCA.......................................................................................23
3.3 The Digital Millennium Copyright Act 1998.................................................................25
   3.3.1 The safe harbor.....................................................................................................27
       3.3.1.1 Transitory network communication.............................................................27
       3.3.1.2 System caching...........................................................................................28
       3.3.1.3 Information residing on systems or networks at direction of users............29
3.3.1.4 Information location tools........................................................................................................ 30
3.3.2 The notice and takedown procedure............................................................................................ 30
3.3.3 Case law.................................................................................................................................... 33
3.3.4 Evaluating the DMCA................................................................................................................ 35
3.3.5 Conclusion................................................................................................................................ 39

Chapter 4: The EU Approach: E-Commerce Directive 2000
4.1 Introduction.................................................................................................................................. 41
4.2 E-Commerce Directive 2000......................................................................................................... 42
4.3 Liability of intermediary service providers.................................................................................. 43
  4.2.2.1 Mere conduit......................................................................................................................... 44
  4.2.2.2 Cache.................................................................................................................................. 45
  4.2.2.3 Hosting............................................................................................................................... 46
  4.2.2.4 No general obligation to monitor....................................................................................... 47
4.4 Case law....................................................................................................................................... 48
4.5 Evaluating the E-Commerce Directive......................................................................................... 50
4.6 Conclusion.................................................................................................................................... 54

Chapter 5: Analysis of the regulatory frameworks
5.1 Introduction.................................................................................................................................... 55
5.2 Comparison of the systems........................................................................................................... 55
Abstract

In the digital networked environment, copyrighted works are displayed, reproduced or distributed unlawfully from one user to another by only one mouse click. Copyright owners have suffered from high cost of damages from such infringing activities committed easily through the internet networks, so they tend to look for someone who can be responsible for their loss. Internet Service Providers, in this sense, are somewhat relevant to the case of online copyright infringement since the functions that they perform might contribute to, induce, or cause such infringing activities. The controversial issue which might arise here is to what extent
ISPs should be held liable for copyright infringement conducted by others since the main function of ISPs is merely providing data conduit of a transmission of copyrighted information. To hold ISPs liable for third-party copyright infringement regardless of reasonable foundation is not justifiable. The US and EU enacted regulations with regard to the limitations of liability concerning ISP liability for third-party copyright infringement which intends to combat online copyright infringement, and provide legal certainty for ISPs where they comply with the conditions set forth in the regulations. In a nutshell, the regulations establish what can constitute liability so that ISPs will know their rights and obligations when they have to deal with copyright infringement committed by others.

Chapter 1
Introduction

1.1 Study Background
An amazing capability of the internet to promote the exchange of knowledge, information, and ideas on the global scale has surely revamped the way people interact.\(^1\) The greatest advantage of the internet is that it plays an essentially crucial role as a medium which has the ability to enable people around the world to obtain great quantities of information within seconds just

\(^1\) The matter of face-to-face present is not necessary anymore for the interaction between people.
by one mouse click. In this way, the internet has given power to people to transmit and
duplicate a vast amount of data or information, including copyrighted materials. Due to the
fact that in the digital network environment the material is rarely transmitted directly from the
originator to the end-user, usually a range of providers act as go-betweens for content creators
and consumers. Such go-betweens are hosting service providers, communications or network
providers, and access providers who play a role as intermediaries by providing the venues for
internet users to download, upload post or transfer such materials. In this thesis the Internet
Service Provider (ISP) will be the focal point of studying. ISP is one type of such intermediaries
providing internet access services to their subscribers in exchange for a fee. Additionally, they
provide a variety of services, including, data-storage for their customers on newsgroup servers
or World Wide Web servers.

With regard to copyright law, copyrighted works transmitted and duplicated through the
digital networked environment without the permission of copyright owners is considered as a
violation of the copyright. A number of copyright infringing activities conducted through the
online world extremely increases because the main characteristics of the internet is to facilitate
such fraudulent activities. At present, the traditional way to deal with copyright infringement is
no longer effective since those who directly conduct unlawful acts seem to be anonymous and
undetectable. As a result, copyright owners have sought a way to compensate their damages

Law & Policy, Vol. 6, No. 1. p. 31.
3 K. Koelman, ‘Online Intermediary Liability’, in Hugenholtz (ed.) Copyright and Electronic Commerce: Legal
p. 7.
4 Internet Service Providers offer a wide spectrum of information processing service such as search service,
chats, forums, hosting, storage, payment, marketing, and design service.
5 B. Bolin & D. Tysver, ISP Liability, at http://www.bitlaw.com/internet/isp.html, last visited on 30 May 2009. See also
R. Mann & S. Belzley, (2005), ‘The Promise of Internet Intermediary Liability’, William and Mary Law Review,
Vol. 47. pp.11-14.
6 See ibid.
7 US Copyright Act of 1976.
8 Exclusive owner rights, contained in U.S. s106 (as codified and amended at 17 USC
section 101-1010 (1998)) are as follow: (1) copying the copyright work; (2) preparing derivative works; (3)
distributing copies of the works; (4) performing the works publicly; and (5) displaying the work publicly.
9 B. Mercurio, (2002), ‘Internet Service Provider Liability for Copyright Infringements of Subscribers: A
Comparison of the American and Australian Efforts to Combat the Uncertainty’, Murdoch University Electronic
by looking at ISPs as potential targets to be sued. In this relation, from the copyright owner’s perspective, ISPs have the ability to determine whether infringing material is being transmitted over their networks and stored on their servers. Moreover, ISPs have been dragged into the center of copyright owners’ attention as potential defendants since their roles as a middle-man are believed that, to some extent, they might be responsible for infringing activities conducted by their subscribers. In this regard, according to the legal doctrines of copyright law, ISPs could be held liable on direct liability, contributory liability or vicarious liability for the copyright infringement committed by their subscribers. Furthermore, ISPs are easy to be identified and deemed to have deep pockets. Moreover, ISPs are in a good position to supervise how their subscribers make use of the internet. Accordingly, these factors make ISPs potentially engage in the copyright infringement in the eyes of the law.

On the other hand, one might argue that it is not justifiable to impose liability upon ISPs for the illegal activities performed by others. In addition, to impose obligations upon ISPs to monitor/police/supervise activities going on through the internet network is burdensome and impractical since the volume of material transmitted over their systems is too large to monitor. Also, even if ISPs are willing and able to monitor materials on their own systems, it could not necessary identify infringing materials. This controversial issue has been discussed over decades and there has been a lot of ink spilt on this issue (either support ISP liability or oppose ISP liability). Regarding to one who supports ISP liability, ISPs seem to be in a vulnerable

---

10 See ibid.
12 See infra Chapter 3.
13 See supra note 9 (citing T. Casey, p. 101).
position if they have to bear a burden of monitoring the internet traffic where “trillions of bits of information representing millions of messages and files travel through networks each day”\textsuperscript{15}. It is therefore virtually impossible for ISPs of large systems to review every message transmitted or file uploaded. Moreover, it is relatively unjustifiable that ISPs are seen as potential defendants just because they simply provide services for their subscribers. On the contrary, for those who oppose ISP liability, ISPs are believed to bear responsibility for the copyright infringement occurred through their systems in certain circumstances since they are in a good position to supervise their subscribers and might have known that their subscribers make use of the internet unlawfully. As a result, many countries\textsuperscript{16} have become aware of this issue and seek a way to compromise between copyright owners’ interest and the limitations of liability for ISPs. This thesis concentrates on US and EU regulatory frameworks on the limitations of liability for ISPs. According to US copyright law, US has responded to this issue through an enactment of the Digital Millennium Copyright Act 1998\textsuperscript{17} providing the safe harbor for ISPs to be exempted from being held liable where they follow the procedure set forth according to the Act. The EU has enacted the E-Commerce Directive\textsuperscript{18} which contains provisions concerning the liability of intermediaries. Similarly to the DMCA; the Directive provides shelter for ISPs to be excluded from being held liable in certain conditions. Consequently, this thesis will focus on the liability of ISPs; whether it is justifiable to hold ISPs liable for the copyright infringement committed by others and if so to what extent ISPs should be responsible for third-party copyright infringement. The research question, methodology, and structure of the thesis will be addressed below.

1.2 Research Question

\textsuperscript{16}For example Australia Copyright Amendment (Digital Agenda) Act 2000, India Information Technology Act 2000, Singapore Copyright Amendment Act 2005, HK copyright (Amendment) Bill (proposed, 2007), New Zealand Copyright (New Technologies) Amendment Act 2008.
\textsuperscript{17}\textit{See infra} Chapter 3, paragraph 3.3.
\textsuperscript{18}\textit{See infra} Chapter 3, paragraph 3.2.
The main research question which will be examined in this thesis is “to what extent should ISPs be held liable for third-party copyright infringement? Furthermore, in order to respond to the research question coherently and to be able to draw conclusions regarding the central question, several sub questions will be examined.

**Sub questions:**

- Should ISPs be held liable for copyright infringements conducted by others?
- What legislation is applicable to ISP liability in the US?
- What legislation is applicable to ISP liability in the EU?
- What are the differences in US and EU legislation regarding ISP liability for third-party copyright infringements?

**1.3 Methodology**

The methodology of this thesis will be a comparative literature study. The main regulatory framework on liability of ISPs of US and EU will be the subject of examination. In order to effectively respond to the research question, the concise overview of the general issues relating to the research question will be provided, namely, the meaning of ISP, how ISPs are involved in copyright infringement conducted by others, why ISPs are deemed as potential defendants in copyright infringement cases, and on what basis ISPs can be held liable? Such general issues will be deliberated in order to pave the way to the in-depth examination of the regulatory frameworks of ISP liability in US and EU. After that, the regulatory frameworks with regard to ISP liability in both regimes will be harmoniously emphasized and compared. The comparison of the legal regimes will result in the analyses of the advantages and drawbacks of the different approaches. Furthermore, to make the analysis complete, case laws will be examined. Finally, a conclusion will be drawn from the analysis of comparative study, and some proposals as well as suggestions will be proposed to improve US as well as EU legislation on ISP liability.

**1.4 Structure of the thesis**

The thesis consists of 6 Chapters. The first chapter deals with the introduction composing of the study background, the research question, and methodology to conduct the research and
structure of the thesis. The second chapter provides briefly insight into general issues with regard to ISP liability for third-party copyright infringement as an introduction to an elaborate analysis of the US and EU regulatory frameworks in the third chapter. The third chapter particularly concentrates on the US regulatory regime which will be divided into two eras. First, the legal doctrines of copyright law that courts applied in each case as a ground of accountability to hold ISPs liable in the era of Pre-DMCA will be described. In this way, the common law principles will be examined and evaluated in order to build up the understanding of the situation on ISP liability in the period of time when DMCA had not yet been implemented. Second, the DMCA will be stressed especially on the provisions concerning the limitations of ISP liability. In the fourth chapter, the EU regulatory framework mainly consisting of the E-Commerce Directive will be examined particularly section 4 of the E-Commerce Directive regarding Liability of intermediary service providers. After that, both regulatory frameworks will be examined and evaluated in each chapter. Next, the fifth chapter emphasizes the comparative study differences between the US and EU regulatory frameworks on ISP liability, and analyses each regulatory framework in such a way that the research question can be addressed. Additionally, pro(s) and con(s) of the existing frameworks will be pointed out which will serve as a basis for drawing conclusions and presenting some fruitful proposals/recommendation to enhance both regulatory frameworks in the final chapter.

Chapter 2
General issues of ISP liability for third-party copyright infringement

2.1 Introduction
This chapter will provide a short background on ISP liability for third-party copyright infringement and briefly gives a general idea how ISPs could be involve in copyright infringement committed by others. It will start with the definition of online intermediaries, which vary depending on the role they play. The next paragraph will especially deal with the reasons why ISPs feasibly can be seen as potential defendants in lawsuits. The next paragraph will provide an overview on kinds of liability that are applicable in the case of ISP liability for
third-party copyright infringement. Finally, the last paragraph will describe kinds of potential liability that ISPs might be held liable.

2.2 What is an Internet Service Provider?

Online intermediaries come in several forms, namely Internet Service Providers (ISPs), Bulletin Board Systems (BBSs), Network operators, Access providers, Host service providers, Information location tool providers, et cetera. Each of these actors has a role to play differently in the digital networked environment. According to the different functional roles of online intermediaries, the following type of online intermediaries can be categorized:

1) Network operator: providing the technical facilities for the transmission of information such as cable, routers and switches.

2) Access provider: providing users with access to the internet. Users connect to the internet through their access providers' servers.

3) Information location tool providers: providing online tools used for finding information that resides in another Web sites such as Yahoo!, Alta Vista, Google, etc. There are two types of search engines, namely, automated search engines and search engines that rely upon people to review and catalogue Web sites.

4) Host service providers: services in which users may rent Web sites space, set up Web pages, and upload content, such as software, text, graphics, or sounds. Hosting services may include online exchange also, like bulletin board and chat rooms which allows direct communication in real time.

These different online intermediaries play different roles when internet users wish to use the internet common ways such as surfing the net, or uploading and downloading materials. In

---


20 See ibid.
order to do so, internet users first need to connect to the network via access providers. Then, assisted by browser software and often by an information location tool, internet users will identify and contact servers operated by host service providers where web pages they wish to contact are located. Depending on the type of web page, in addition to browsing the page, internet users may be able to request information, upload materials, and download files to their personal computers. Internet users will also be able to connect to the newsgroup hosted by a host service provider. In order to participate in the newsgroup, internet users will send a message that will be posted in the newsgroup. In addition, they will be able to read the posted messages sent by other internet users.21

To make it simple, the term ISPs will be used through this thesis which aims to cover a wide range of companies and organizations that provide their subscribers with different facilities, ranging from providing access to the internet, to giving their subscribers the means to make documents publicly available over the internet. For example, ISPs may provide their subscribers with more than just an email account and access to the web. They may also give them the right to upload files, software, text, sound, etc. to the ISP's publicly accessible servers.22

2.3 Reasons for pursuing claim against Internet Service Provider23

It is rational for ISPs to bear some responsibility for copyright infringing activities conducted by others. With regard to copyright infringement, as mentioned, the expansion of the internet


makes it easy for anyone who wishes to upload, download, post, disseminate or transmit copyrighted materials. ISPs play a crucial role as a middle man to provide and facilitate those activities. As ISPs, to some extent, are involved in those activities, copyright owners put ISPs high on the list as potential defendants in online infringement lawsuits. There are several reasons why aggrieved parties may decide to pursue action against ISPs rather than subscribers who are direct infringers.

First, in the online world, identity is hidden and malicious-minded people can violate the copyright anonymously and from any territorial area. Therefore, it is tricky for copyright owners to sue them. In addition, to bring a lawsuit against defendants who are not in the plaintiff’s home jurisdiction is burdensome in several aspects. On the contrary, ISPs are identifiable and easy to be located. It is therefore relatively easier for copyright owners to pin point the location of ISPs instead of their subscribers. Second, copyright owners are looking for deep pockets to pay high damages. It is obvious that the internet users are not the right target to sue since in general, their financial support is less sufficient to cover damages. Hence, it is not worth the time and money for copyright owners to bring a lawsuit against them. Finally, copyright owners will often wish to bring an action against a person in his home jurisdiction, and in many cases the only possible candidate will be ISPs. However, to hold ISPs liable for the illegal actions of others needs legal doctrines which offer plausible support for the general idea of ISP liability. Copyright owners, in this sense, might wish to have a particular regulation which can be the basis of accountability in order to sue ISPs. The following paragraph will describe the type of liability that can be applied to copyright infringement involving ISPs and their users.

### 2.4 Types of liability

According to the Copyright law, basically, copyright owners have exclusive right to exclude others from reproducing or distributing their copyrighted works without authorization. One who violates those rights will be held directly liable for copyright infringement as a direct infringer. On the other hand, as for the issue of ISP liability, it comes in the form that ISPs have to bear responsibility for an infringement conducted by third parties. To make it clear, the issue
of ISP liability deals with liability that ISPs truly act as a passive conduit, meaning that they do not initiate the infringing activity by themselves, otherwise they would be held directly liable. Liability for harm done by others is generally governed by tort law.\textsuperscript{24} In this relation, in order for ISPs to be responsible for an infringement conducted by others, they must have actual knowledge or constructive knowledge (awareness of facts or circumstances of infringing activity) so that they can be held vicariously or contributory liable. In this light, the knowledge of ISPs is fundamental because it is the key whether to impose liability upon ISPs. Basically, two kinds of liability are distinguished.

\textbf{2.4.1 Strict liability (no-fault liability)}

The concept of strict liability (direct liability) is that ISPs will be held liable regardless of their knowledge and control over materials disseminated through their systems.\textsuperscript{25} This liability is rigid since ISPs might be considered as infringers, even though they do not have any knowledge of infringing activity or any control over certain materials. It also indirectly imposes an obligation of policing their system upon ISPs since they have to be aware of infringing activity which may be occurring through their networks.\textsuperscript{26}

\textbf{2.4.2 With-fault liability}

According to the with-fault standard, ISPs will be held liable whenever they intentionally or negligently violate the right of others with knowledge of infringing activity.\textsuperscript{27} The knowledge of infringing activity can be divided into two levels; actual knowledge and constructive knowledge. The actual knowledge is apparent where ISPs know that there is infringing materials disseminated, or there is infringing activity performed through their systems. Under the constructive knowledge, the law may determine if ISPs have reason to know that materials disseminated through their networks violate someone’s right, or ISPs have clues that can reasonably assume of infringing activity, and then ISPs will be held liable. In relation to with-

\begin{itemize}
  \item \textsuperscript{24} See supra note 3, K. Koelman, p.8.
  \item \textsuperscript{25} See supra note 19, R. Julia-Barcelo, p. 10.
  \item \textsuperscript{26} See supra note 19, P. Basicrocchi, p.114.
  \item \textsuperscript{27} See supra note 3, K. Koelman, p.8..
\end{itemize}
fault liability, ISPs will be held liable for vicarious liability where they have the right and the ability to control an infringer and they could gain benefit directly from the infringement. Moreover, ISPs will be held liable for contributory liability where they know or have reason to know of infringement, facilitate, or induce such infringement.\textsuperscript{28}

\textbf{2.5 Areas of potential liability}

This thesis focuses merely on ISP liability for copyright infringement. However, there are various types of violations that can occur through the use of online intermediaries’ facilities that concern with not only one civil law, but also criminal law. This paragraph briefly describes various infringements as follows:

1) \textit{Copyright material}: The infringing act occurs when certain copyrighted files are posted on web pages where it allows such files to be downloaded, transmitted, or distributed through the internet network without the authorization of the copyright owner.

2) \textit{Illegal and harmful content}: The infringing act may occur where certain materials containing pornography, racist, or terrorist contents are disseminated through the internet network.

3) \textit{Private and defamatory material}: The infringing act may occur when private materials such as private pictures or private text could be posted on the web page, bulletin board, chat room, etc. and made publicly available without permission of owners of such materials. Moreover, the same act may occur with defamatory materials when a libelous text could be posted through the internet network.

4) \textit{Trade secrets}: The infringing act may occur when employees disclose business secret or confidential information which may be used in trade or business.

5) \textit{Misrepresentation}: This might happen when someone provides false or incorrect information which could be disseminated through the internet network and cause damage to a third party.\textsuperscript{29}

\textsuperscript{28} \textit{See infra} chapter 3.
\textsuperscript{29} \textit{See supra} note 19, R. Julia-Barcelo, pp. 5-6.
In summary, this briefly chapter purports to give a basic insight in order to pave a way to following chapters which will deliberately describe ISP liability for third-party copyright infringement in US and EU regimes. To this end, ISPs can be seen as potential defendants in lawsuit concerning copyright infringement conducted by others since there are types of liability that can possibly be applied in this situation. Moreover, as stated above, ISPs may involve in various kinds of potential liability. In following chapters, the thesis will be processed by describing the issue of ISP liability in different regimes, as well as explaining how different regimes codify this matter into their legislations.

Chapter 3
The U.S. Approach: The Digital Millennium Copyright Act 1998

3.1 Introduction
The exponential growth of the internet makes the unauthorized transmission and duplication of copyrighted works easier. The US takes the issue of copyright infringement as a prime concern because the violation of the copyright which costs a high damages to copyright owners is
increasing consistently. The internet has made it harder to trace actual wrongdoers. As a result, ISPs have become a center of attention to be sued because of their identifiable location and reliable financial status. Apparently, in the US regime, the copyrighted works are protected by the Copyright Act of 1976. The Copyright Act states that copyright owners have exclusive rights which are; (1) copying the copyright work; (2) preparing derivative works; (3) distributing copies of the works; (4) performing the works publicly; and (5) displaying the work publicly. Copyright owners can exercise these rights exclusively without the interference of others. However, as aforementioned, copyrighted materials are transmitted and duplicated in different ways in the digital networked environment. As a result, traditional way to protect the exclusive rights of copyright owners is less effective. Therefore, the DMCA was enacted with the purpose of balancing the interest between ISPs and copyright owners, as well as providing the extent of liability which can be applied to ISPs in case of third-party copyright infringement. This chapter will divide rules that govern ISP liability into two eras. The first paragraph will deal with the situation of ISP liability for third-party copyright infringement in the era that the DMCA had not yet been implemented. Hence, significant rules that governed ISP liability were legal doctrines from copyright law which had been adopted from tort law. Then, the second paragraph will concentrate on the DMCA era. This section will provide provisions established in the DMCA which are particularly relevant to the limitations of ISP liability.

3.2 Pre-Digital Millennium Copyright Act of 1998 (Pre-DMCA)

Before the enactment of the DMCA which establishes provisions on the limitations of ISP liability, courts held ISPs liable for copyright infringement on the grounds of common-law principles. With regard to the Copyright Act of 1976, a person who violates any one of exclusive rights would be held directly liable for copyright infringement. However, even if the Copyright Act did not explicitly render anyone liable for infringement committed by others, under certain circumstances, ISPs would possibly be held liable for the infringing acts of others under the

30 The music industry, worth over $US40 billion annually, has suffered considerably from the internet boom, with the Recording Industry Association of America (RIAA) estimating that over $US4.5 billion annually is lost to worldwide music piracy. See The World Sound Recording Market, RIAA Publication, at http://www.riaa.com/MD-World.cfm, last visited on 13 May 2009.
legal doctrines of secondary liability which are vicarious and contributory liability. These legal doctrines will be discussed below.

3.2.1 Kind of liability applicable to ISPs under Pre-DMCA case law

3.2.1.1 Direct liability

Direct copyright infringement consists of the unauthorized exercise of one of the exclusive rights of copyright owners provided in section 106 of the Copyright Act. Two requirements must be satisfied in order to present a case for direct liability: (1) the plaintiff must show ownership of the allegedly infringing material; and (2) the plaintiff must demonstrate that alleged infringers violate an exclusive right granted to copyright owners.

In some cases, ISPs have been sued for direct copyright infringement as long as they were considered to have made unauthorized reproductions only by operating the servers and the networks through which the copies were made even if they had no knowledge of infringing copies. That is, court could hold ISPs liable for their subscribers’ behavior by concluding that ISPs commit copyright infringement simply by providing basic internet service to infringing subscribers. This outcome seemed plausible because ISPs automatically and routinely reproduce and distribute copyright materials in response to subscriber requests. Subscribers upload materials to web pages by instructing ISP’s computer to make and store copies of uploaded materials. The ISP’s computer

---

33 The Copyright Act of 1997 does not explicitly recognize the possibility of indirect liability. Nevertheless, courts have held third parties liable for copyright infringement under two long-standing common law doctrines: contributory liability and vicarious liability. See the example cases, Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2nd 304, 307 (2nd Cir.1964) (holding department store vicariously liable for copyright infringement of record sales concessionaire); Fonovisa, Inc., v. Cherry Auction, Inc., 76 F. 3d 259, 261-64 (9th Cir. 1996) (holding operator of swap meet vicariously liable for copyright infringement of boot renters); Gershwin Publ’g Corp. v. Columbia Artists Management, Inc., 443 F. 2d 1159, 1162-63 (2nd Cir 1971) (holding liable for infringing performances by musician).

34 For further detail; see A. Yen, (2002-03), ‘Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability and the First Amendment’, Geotrgtown Law Journal, Vol. 88, No. 1833 (He analyzed the legal doctrines of Copyright Act, direct, vicarious and contributory liability), pp.8-45.


36 To prove the copyright element, the plaintiff may either produce direct evidence that defendant copied the plaintiff’s material, or create an interference that copying occurred by showing that the defendant had access to the protected work, and the two works are similar. Once the plaintiff has satisfied these requirements, the plaintiff can then establish direct infringement by proving the defendant used the alleged copies in ways described under Section 106. See Playboy Enters, Inc. v. Russ Hardenburgh, 982 F. Supp. 503,508 (N.D. Ohio 1997), (citing Feist Publications, Inc. v. Rural Tel. Serve. Co., 499 U.S. 340, 361 (1991)).
then makes copies of materials every time a person view subscribers’ web page and sends those copies through the internet to viewing parties. In addition, whenever subscribers download information from the internet, their ISPs receive copies of copyrighted materials and send that materials to subscribers. The landmark case where an ISP was held directly liable for copyright infringement is Playboy Enters., v. Frena. It was the first case and the only case which considered the issues which is relevant to this theory most extensively. Courts of subsequent case law have discredited it. For example, in the case Religious Technology Center v. Netcom On-line Communication Service, Inc.

**Playboy Enterprises, Inc. v. Frena**

In Frena, the defendant operated a subscription computer bulletin board service (BBS) where Frena’s subscribers can download and upload materials stored on Frena’s computer. Playboy sued Frena on the ground that Frena violated its exclusive copyright by displaying and distributing its photographs when subscribers posted copyrighted photographs on the services. Frena claimed that the ISP itself had not uploaded any of playboy’s images on BBS, but that photographs were only posted by its subscribers. Moreover, as soon as Frena became aware of infringing activity, those infringing images were removed from BBS. The court held that the BBS computer’s automatic copying, storage, and distribution of Playboy’s images infringed Playboy’s exclusive copyright rights. Moreover, the court disregarded the objection of Frena that it did

---

37 The internet operates by making and sending copies of information from one computer to another. Material viewed on a subscriber’s home page is generally stored on ISP’s computer. Internet users view the subscriber’s home page by sending the request to relevant files to the ISP’s computer. That computer automatically responds by making a copy of the files stored by the subscriber and transmitting the files over the internet to the requesting party. In many cases, those files also pass through intermediate computers on the internet, each of which may make a copy of the files before transmitting them further along the network. Thus, the use of copyrighted material on subscriber’s web page implies making and distributing copies of the materials, see P. Gralla, ‘How the internet works’ (Millennium ed. 1999).

38 Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552 ( M.D. Fla. 1993)


40 See discuss below infra 3.2.2.

41 See summary of the case, supra note 34, A. Yen, pp.8-9.

42 See Playboy Enters., Inc. v. Frena at 1554 (describing how Frena’s BBS operated). A bulletin board service (BBS) stored and distribute files for its subscribers. Subscribers generally use a modem to connect to the BBS. Once connected, the subscriber can download files on the BBS computer or upload files that the subscriber wishes to leave for others to see.

43 See ibid. at 1556-57.
not upload those infringing images by itself and did not know that those images have resided on the BBS. The court strictly established the statutory statement that "It does not matter that defendant Frena may have been unaware of the copyright infringement. Intent to infringe is not needed to find copyright infringement. Intent or knowledge is not an element of infringement, and thus even an innocent infringer is liable for infringement."  

3.2.1.2 Secondary liability

Secondary liability is the imposition of liability on a defendant who did not directly commit the violation at issue which originated in tort law. Secondary liability comes in two forms: vicarious liability and contributory liability. In many cases, ISPs have been sued for contributory infringement which is to say, for inducing, causing and providing the means to carry out the infringement, knowing or having reason to know of the infringement. In other cases ISPs have been sued for vicarious liability where they are capable of controlling their subscribers and profit financially from the infringement.

3.2.1.2.1 Vicarious liability

Although the copyright Act does not explicitly establish vicarious liability, U.S. courts have consistently imposed vicarious liability on the defendant when the defendant had the right and the ability to supervise the infringer’s act and received financial benefits directly from the infringement. Hence, ISPs may be held liable for vicarious liability since ISPs have a certain relationship to subscribers and could gain financial interest from the infringement. Nevertheless, courts hesitate to impose vicarious liability upon ISPs because of the facts that ISPs can hardly control their subscribers and ISPs do not profit financially from the unlawful act of their subscribers directly. Only two courts have considered the issue of ISP vicarious liability.

44 See ibid. at 1559.
46 See supra note 32, S. Högberg.
47 See supra note 33.
48 See Netcom, 907 F. Supp. 1361, 1357-77 (finding the ISP not liable for vicarious liability, even if monitoring was possible, since the financial benefit could not be shown); Roy Export Co. v. Trustee of Columbia University, 344 F. Supp. 1350, 1353 (S.D.N.Y. 1972) (finding the University was not vicariously be held liable for the screening of bootlegged films as it did not receive any financial interest).
In both cases, ISPs could not be held vicariously liable as the two requirements could not be fulfilled.

**Religious Technology Center v. Netcom On-line Communication Service, Inc.**

The plaintiffs, Religious Technology Center and Bridge Publications, Inc. owed copyright in the writing of L. Ron Hubbard, founder of the Church of Scientology. The plaintiffs sued Dennis Erlich, a former member of the Church of Scientology on the basis that he made available a number of postings to the internet through a computer Bulletin Board Service (BBS). His postings consisted of the excerpt from the copyrighted writing of the plaintiffs and the critical posting which are related to the Church. The plaintiffs claimed that Erlich’s posting violated their copyright. They contacted Thomas Klemesrud, the operator of the BBS, and Netcom, the ISP for the BBS, to terminate Erlich’s internet access. Klemesrud and Netcom refused to do so. Therefore the plaintiffs sued them because they were directly, vicariously and contributory liable for copyright infringement. To understand this case, simplifying the technical relationship among Erlich and Klemesrud is crucial. Erlich did not gain access to the internet directly through Netcom. Instead, Erlich contracted with Klemesrud for the right to post messages on Klemesrud’ BBS. Klemesrud in turn arranged for access to the internet through Netcom. Therefore, the plaintiffs claim against Netcom involved in infringement committed by a customer of Netcom’s subscriber and not an infringement committed by the subscriber himself. The court considered two facts which existed in the case regarding Netcom’s ability to supervise Erlich and Netcom’s financial interest in Erlich’s infringement. The court ruled that even though Netcom might have had the ability to supervise, Netcom did not gain financial benefit directly from Erlich’s infringement. Therefore Netcom could not be held vicariously liable. To hold ISPs vicariously liable, courts are likely to be strict in the requirement of financial interests that ISPs could obtain from infringing activities conducted by their subscribers, but merely the flat fee that ISPs charge their customers by using their services cannot be seen as beneficial interests that ISPs obtain directly from infringements. The second case considering the issue of ISP vicarious liability is Marobie-FL, Inc. v. National Association of Fire Equipment

---

Similarly to Netcom the court refused to hold the ISP vicariously liable, but on slightly different facts.

**Marobie-FL, Inc. v. National Association of Fire Equipment Distributors**

The plaintiff Marobie owned copyright in clip art developed for use by the fire service industry. The defendant, National Association of Fire Equipment Distributors (NAFED), had a web page on the internet which was hosted by the servers of its ISP, Northwest Nexus, Inc. Due to the fact that NAFED, through its agent, copied the copyrighted images of Marobie on to its webpage, it made such copyrighted images available to be freely accessed by internet users who viewed its webpage and those images were somehow downloaded by internet users. The plaintiff sued NAFED for direct copyright infringement and Northwest, its ISP, for direct, vicarious and contributory copyright infringement. In this case the Northern District of Illinois considered the result the same as the Netcom case, however; there are different facts that make the two cases distinct. In the Marobie case, The ISP, Northwest was being sued for direct infringement conducted by its subscriber NAFED. On the other hand, in the Netcom case, ISP Netcome was being sued for direct infringement performed by the customer Erlich of its subscribers Klemesrud. As a result the relationship between Netcom and Erlich is so distant that Netcom could not supervise. Therefore, Netcom was not liable for vicarious liability. To the contrary, in the former case the relationship between Northwest and its subscriber NAFED is close enough to justify vicarious liability, yet the court considered to follow Netcom case stating that the facts regarding supervision and the flat fee that Northwest gained from NAFED made a finding of financial interest impossible.

### 3.2.1.2.2 Contributory liability

The Copyright Act grants copyright owners not only the right to exercise exclusive rights, but also the right to authorize the exercise of those rights. The authorization right was

---

52 See 17 U.S.C. Section 106 (“The owner of copyright under this title has the exclusive rights to do and to authorize any of the following . . . .”)

“intended to avoid any question as to the liability of contributory infringers” - those who do not exercise the copyright owner’s right themselves, but authorize others to do so. 53 Other than the reference to the authorization right, the Copyright act does not mention or define contributory infringement. 54 Nevertheless, contributory liability is a judge-made doctrine which is similar to vicarious liability. According to the courts, “one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a contributory infringer.” 55 Contributory liability requires ISPs to have actual knowledge and strong evidence of the infringing activity conducted by others. It is therefore a burden of the plaintiff to prove the knowledge of ISPs, as well as, to provide strong evidence that ISPs know or should have known of the infringement after receiving the notice from the plaintiff. This theory was applied in Sega Enterprises v. MAPHIA. 56

**Sega Enterprises v. MAPHIA**

According to this case, the Bulletin board operator, MAPHIA, allowed its users to upload and download into their computers Sega copyrighted videogames. The court held MAPHIA contributory liable because of the fact that MAPHIA had knowledge that its users copied Sega videogames. Moreover, MAPHIA caused and contributed to the infringing activities by actively soliciting users to upload unauthorized games, and by providing road maps on their BBS for easy identification of Sega games available for downloading. In this case, it is relatively evident that MAPHIA was liable for contributory copyright infringement because it was obvious that they had knowledge and the intention to contribute to the infringement.

### 3.2.2 Analysis of rules governing ISP liability for copyright infringement in the era of Pre-DMCA

54 See ibid.
Courts have begun to develop the law governing ISP liability for third-party copyright infringement along a sensible line, but there is no guarantee that those common law principles will be followed in the future.\footnote{See supra note 34, A. Yen, p.45.} First, it is unlikely that direct liability for copyright infringement will be applied to ISPs due to extreme and unreasonable liability it created.\footnote{B. Mercurio, (2002), ‘Internet Service Provider Liability for Copyright Infringements of Subscribers: A Comparison of the American and Australian Efforts to Combat the Uncertainty’, Murdoch University Electronic Journal of Law, Vol. 9, No. 4. (citing Religious Technology Center v. Netcom, 907 F. Supp. 1361(N.D. Cal. 1995); Marobie-FL,Inc. v. National Association of Fire Equipment Distributors, 983 F. Supp. 1167, 1178 (N.D. Ill. 1997); Sega Enterprises v. Maphia, 948 F. Supp. 923, 931-32 n.5 (N.D. Cal. 1996)).} According to the Frena case where the court ruled that the BBS operator was liable simply for passively accepting uploads from subscribers and sending copies of uploads to other subscribers, then ISPs should be similarly liable.\footnote{See supra note 34, A. Yen, p.45.} As a result, several subsequent cases have discredited this theory. For instance, just two years after the Frena case, in the leading case of Religious Technology Center v. Netcom On-line Communication Service, Inc, the court considered the claim ISP Netcom was directly liable for duplicating and disseminating allegedly infringing postings made to the internet by Dennis Erlich, a BBS user and rejected the Frena approach, writing that “although copyright is a strict liability statute, there should be some element of volition or causation which is lacking where a defendant’s system is merely used to create a copy by a third party”.\footnote{See supra note 34, A. Yen, p.45.} The court continued, “where the infringing subscriber is clearly directly liable for the same act, it does not make sense to adopt a rule that could lead to the liability of countless parties whose role in the infringement is nothing more than setting up and operating the system that is necessary for the functioning of the internet.”\footnote{See ibid. at 1372-73.} It is therefore difficult and problematic to conclude that ISPs should be or could be held liable for simply providing the service to infringing subscribers. Moreover, easily holding ISPs liable for direct infringement contributes to the adverse effects on the free flow of information on the internet and would ultimately drive ISPs out of business.\footnote{See supra note 15, White Paper. pp. 115-116.} Second, vicarious liability is relatively weak to hold ISPs liable since the relationship between ISPs and subscribers is not close enough for ISPs to have the right and the ability to supervise their subscribers. Furthermore, to impose obligations upon
ISPs to monitor/screen/control the behavior of their subscribers is overwhelmingly burdensome and impractical. According to the Netcom case, although the court concluded that Netcom might have had the ability to supervise Erlich because the court considered the existing fact that Netcom could have employed the software modification easily allowing Netcom to identify postings that came from particular people or contained certain words, the ISP received a flat fee for internet service, it does not gain financial interest directly from the infringing activity of their subscribers. Thus, vicarious liability is likely to be refused by courts. Nevertheless, it would be wrong to conclude that other courts have followed Netcom and Marobie because only two courts have addressed the issue concerning vicarious liability; the issue regarding vicarious liability may remain open in most jurisdictions.\footnote{See supra note 34, A. Yen. p. 15.}

Thirdly, contributory liability seems to be a sensible ground to hold ISPs liable since it requires knowledge of ISPs and the reaction upon receiving a notification from copyright owners seems to be a rational ground to prove knowledge of ISPs. However, there is no standard of actual knowledge or constructive knowledge (awareness) of ISPs to determine whether ISPs have actual knowledge of infringing activity or awareness of facts or circumstances that such activity is apparent. In this relation, of course, when ISPs receive notifications from copyright owners, it can imply that ISPs have knowledge, yet ISPs may be informed about allegedly infringing activities which apparently has not yet been verified. It has resulted in controversial issues of whether ISPs have the right to take down allegedly infringing contents posted on the internet, and whether or not ISPs need to assure that the notification from the copyright owner is not a fraudulent one. This implies that ISPs will be at risk when they need to choose between removing non-infringing materials or suspend internet service to subscribers who have not clearly committed copyright infringement. To do so, it potentially creates the problems of freedom of expression as well as increases litigation costs for the innocent party.

In summary, before the enactment of DMCA which contains the safe harbor and the notice and takedown procedure,\footnote{See infra paragraph 3.3.2.} the situation of ISP liability is far from settled. According to the judge-made principles that have been applied in cases concerning ISP liability, ISPs were put in an
uncertain position. That is, ISPs were seen as infringers just because they provided their services regardless of their knowledge. Moreover, ISPs had not known whether they have duty to monitor infringing activities which might occur through their systems. To this end, it can be concluded that ISPs should be held liable for copyright infringement conducted by others, yet uncertainties still remain for ISPs. That is the issue regarding the limitation and/or the extent of ISP liability remained questionable since courts did not establish the scope of ISP liability.

3.3 The Digital Millennium Copyright Act of 1998

Before the implementation of Digital Millennium Copyright Act (hereinafter DMCA), there was no particular regulation on the limitations of ISP liability for third-party copyright infringement. The previous paragraph explains that courts have made decisions to impose liability upon ISPs by applying judge-made legal doctrines which are unclear, inconsistent and sometime ISPs had to excessively bear responsibility of policing infringing activities committed through their systems. The US Online Copyright Infringement Liability Limitation Act was enacted as part of the Digital Millennium Copyright Act (DMCA). The Act adds a new Section 512 to Chapter 5 of the US Copyright Act, which deals with the enforcement of copyrights. Consequently the DMCA was signed into law on 28 December, 1998 aimed to bring U.S. law into compliance with private international law and in particular with the WIPO Copyright Treaty.

“service provider” is defined as “an entity offering transmission, routing, or providing connections for digital online communication, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the material as sent or received” or, more widely, “a provider of online services or network access, or the operator of facilities thereof.” The DMCA creates four new limitations on ISP liability for copyright

---

65 Public Law 105-308-0CT. 28, 1998.
66 The WIPO Copyright Treaty(WCT), concluded in 1996, recognizes the need to maintain a balance between the rights of authors and the larger public interest, particularly education, research and access to information in updating international copyright norms to respond to challenges arising from advance in information and communications technologies, including global digital networks; see WIPO Copyright Treaty, Dec. 20, 1996, WIPO Doc. CRNR/DC/94, available at http://groups.csail.mit.edu/mac/classes/6.805/articles/int-prop/wipo-copyright.html, last visited on 23 June 2009.
67 DMCA, section 512(k)(1)(A)
68 See ibid. section 512(k)(1)(B). See further infra chapter 5.
infringement, (a so-called the safe harbor”). The limitations are based on the following four categories of activities conducted by a service provider; transitory communication, system caching, storage of information on systems or networks at direction of users, and information location tools. In this regard, ISP will not be held liable if they perform those activities. Moreover, in order for ISPs to benefit from the safe harbor, they must comply with the procedural requirement (a so-called the notice and takedown procedure) set forth in the Act. Title II of the DMCA was purposed not only to deal with the online copyright infringement but also to particularly provide certainty for ISPs. These instrumental purposes of the enactment of the DMCA were stated in the Joint Explanatory Statement of the Committee of Conference: “Title II preserves strong incentive for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment. At the same time, it provides greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities.” This paragraph will examine section 512 of the DMCA on online copyright liability limitation, providing an explanation of the safe harbor and the notice and takedown procedure. Then, case law judged on the basis of the DMCA will be discussed. Finally, the DMCA will be evaluated.

### 3.3.1 The Safe Harbor

Specifically, Title II limits ISP liability for four general categories of activities stipulated below as four safe harbors. However, in order for ISPs to be shielded from liability for copyright infringement they must follow the conditions set forth in section 512. In return, by complying with the conditions established in the DMCA, ISPs can avoid monetary penalties and disabling injunctions. That is, if their activities fall within the safe harbors, the only penalty that they

---


70 See *ibid* section 512(a).

71 See *ibid* section 512(b).

72 See *ibid* section 512(c).

73 See *ibid* section 512(d).


75 See *infra* paragraph 3.3.2.

76 DMCA. Section 512 (a)-(d); “A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of....”
face is a narrow injunction to block access to individual infringing users.77 Moreover, in order for ISPs to be eligible for taking advantage of these four safe harbors, they have to fulfill simply two requirements.78 First, ISPs must adopt and implement the policy provided for the termination of subscribers who are repeat infringers.79 Second, ISPs must accommodate and do not interfere with standard technical measures designed for detecting and/or eliminating copyright infringement.80 Nevertheless, it is not mandatory for ISPs to be pursuant to the certain conditions provided in section 512, meaning that ISPs who do not follow the safe harbor are not automatically liable. Instead, liability must be proven on the basis of existing law.81 Four categories of activities that fall within the safe harbor will be explained below.

3.3.1.1 Transitory network communication

The first safe harbor is described in section 512(a); ISPs who act only as data conduit for transmitting digital information from one point on a network to another at someone else’s request will not be held liable for copyright infringement. This limitation of liability covers acts of transmission, routing, or providing connection for the information, as well as the intermediate and transient copies that are made automatically in the operation of a network. However, the DMCA establishes the conditions following provision 512(a) that ISPs have to meet in order to benefit from the limitation of liability. To make it clear, ISPs will not be held liable where they do nothing but simply provide their services and act as go-betweens. Thus the ability of ISPs to gain knowledge of infringing activities is non-existent.82 Nevertheless, they still

77 See ibid. Section 512(j)(1)(b).
78 See ibid. Section 512(i)(1)(A)-(B).
79 See ibid. Section 512(i)(1)(A).
80 See ibid. Section 512(i)(1)(B). With regard to copyright infringement, technical tool such as digital watermarking allows copyright owner to track their work across the internet by using web spider technology. Web spider is a program that visit web sites and read their page and other information in order to create entries for a search engine index. The major search engine on the web all have such a program, which is also known as a crawler or a bot. Spiders are typically programmed to visit sites that have been submitted by their owners as new or updated. Entire sites or specific pages can be selectively visited and indexed. Spiders are called spiders because they usually visit many sites in parallel at the same time, their “legs” spanning a large area of the “web.” Spiders can crawl through a site’s pages in several ways. One way is to follow all the hypertext links in each page until all the pages have been read. See http://whatis.techtarget.com/definition/0,,sid9_gci213035,00.html, last visited on 23 July 2009.
81 Legal doctrines of Copyright law.
82 C. Beams, (1999), ‘The Copyright Dilemma Involving Online Service Provider: Problem Solved...for now, 51
need to be certain that they fall within the conditions. The conditions mainly require ISPs not to initiate any activities concerning the copyrighted material. Regarding the conditions in section 512(a)(1)-(5), for instance if ISPs do not initiate the transmission of material, do not select the recipient of the material or do not modify the content of material, they will not be held liable for copyright infringement. In other words, ISPs will be shielded from being held liable as long as they purely remain in conduit position.

3.3.1.2 System caching

The second safe harbor is described in section 512(b)(1)(A)-(C). ISPs will be immunized where they temporarily and automatically retain copies for a limited time of material, which has been made available online by a person other than ISPs, and then transmitted to subscribers at their direction. ISPs store materials so that subsequent materials can be fulfilled by transmitting the retained copies, rather than retrieving such materials from the original source on the network (a so-called caching). The system caching concerns the storage of materials in the longer term than the transitory communications. Hence, the ability of ISPs to gain knowledge or to be aware of infringing activities is more likely (even though the possibility of discovering such activities is still very rare). Similarly to the first safe harbor, in order for ISPs to benefit from the limitation of liability, they must act in accordance with the conditions subsequently set forth in section 512(b)(2). That is, ISP must not modify the content of the material, must comply with the content provider’s rule concerning the refreshing, reloading,

---


83 DMCA. Section 512(a)(1)-(5).

84 See ibid. Section 512(a)(1).

85 See ibid. Section 512(a)(3).

86 See ibid. Section 512(a)(5).

87 See Commerce Rep. (DMCA) H.R. Rep. No.1 105-551, Part 2, 105th Cong., 2nd Sess. (July 22, 1998) p.52, available at, http://gozips.uakron.edu/~dratler/2006cyberlaw/materials/sec512leghist.htm, last visited on 11 June 2009; describes caching “which is used on some networks to increase network performance and to reduce network congestion generally, as well as to reduce congestion and delays to popular sites. This storage is intermediate in the sense that the service provider serves as an intermediary between the originating site and the ultimate user. The material in question is stored on the service provider’s system or network for some period of time to facilitate access by users subsequent to the one who previously sought access to it.”

88 See supra note 82, C. Beams, p. 842.

89 DMCA. Section 512(b)(2)(A)
or other updating of the material\textsuperscript{90}, and must not interfere with the technology regarding the material to return to the content provider.\textsuperscript{91} Moreover, ISPs must limit the access to the stored material only for users who act in accordance with the conditions set by the content provider, such as the condition based on payment of a fee or provision of a password or other information.\textsuperscript{92} Finally, ISPs must respond expeditiously to remove, or disable access to, the material which the content provider make available online without the authorization of the copyright owner upon receiving the notification of claimed infringement.\textsuperscript{93}

3.3.1.3 Information residing on systems or networks at direction of users

The third safe harbor, section 512(c) limits the liability of ISPs where they store the material at the direction of a user (user storage).\textsuperscript{94} According to the term “residing”, it implies that the material must be stored on the system for a longer period of time than system caching.\textsuperscript{95} Thus, knowledge of ISPs regarding infringing activities is much more likely. As a result, to take advantage of this safe harbor, ISPs are required to comply with the conditions set forth in Section 512(c)(1)(A)-(C). Namely, there is no actual knowledge of ISPs that the material on their systems or networks is infringing.\textsuperscript{96} Besides, in the absence of such actual knowledge, ISPs are not aware of facts or circumstances from which infringing activity is evident.\textsuperscript{97} Furthermore, ISPs must not receive a financial benefit directly from the infringing activity where ISPs has the right and the capability to control such activity.\textsuperscript{98} Moreover, upon obtaining such knowledge by receiving the notification of claimed infringements, ISPs must act promptly to remove or disable access to the material.\textsuperscript{99}

\textsuperscript{90} See ibid. Section 512(b)(2)(B).
\textsuperscript{91} See ibid. Section 512(b)(2)(C).
\textsuperscript{92} See ibid. Section 512(b)(2)(D).
\textsuperscript{93} See ibid. Section 512(b)(2)(E).
\textsuperscript{94} See supra note 87. p. 53; listing the examples of user storage “providing server space for a user’s web site, for a chat room, or other forum in which material may be posted at the direction of users” but not including material “that resides on the system or network operated by or for the service provider through its own acts or decision and not at the direction of a user”.
\textsuperscript{95} See supra note 64, C. Beams, p. 843.
\textsuperscript{96} DMCA. Section 512(c)(1)(A)(i).
\textsuperscript{97} See ibid. Section 512(c)(1)(A)(ii).
\textsuperscript{98} See ibid. Section 512(c)(1)(B).
\textsuperscript{99} See ibid. Section 512(c)(1)(C), this is the notice and takedown procedure, see infra paragraph 3.3.2
3.3.1.4 Information location tools

The fourth safe harbor, section 512(d), concerns every form of referrals (hyperlink, search engine, online directory, index, reference, and pointer), provided by ISPs, that can link users to another page. It limits liability for the act of referring or linking users to the site containing the infringing materials by using such information location tools. Similarly to the third safe harbor, ISPs are required to follow the conditions which are essentially the same as conditions applied under the third safe harbor.\(^{100}\)

3.3.2 The Notice and take down procedure

In section 512(b)(2)(E), (c)(1)(C) and (d)(3) the notice and takedown procedure is established. This procedure purports to immunize ISPs where they act as “good citizen”\(^{101}\) by encouraging ISPs to cooperate with copyright owners when they receive a notification of claimed infringement from copyright owners. In this way, upon receiving notifications from copyright owners regarding infringing materials, ISPs must expeditiously remove claimed infringing materials or disable access to those materials. Regarding the procedure, it is somewhat irrelevant to ISPs who act as merely data conduit or ISPs who provide information technology tools as in both cases copyright owners tend to be more equipped to disable infringing materials by attacking the site themselves.\(^{102}\) Moreover, in the former case the ability of ISPs to gain knowledge of infringing activities is almost non-existent, as well as in the latter case, it is not relevant to the storage of materials, but concerning the web page provided by ISPs, that link users to another page. Therefore the notice and takedown procedure is essentially relevant to the safe harbor regarding user storage.\(^{103}\) Furthermore, in order for ISPs to enjoy the limitations of liability, they must designate an agent\(^{104}\) to receive notifications of claimed infringement by making substantial information available on their websites, including a location

\(^{100}\) Section 512(d)(1)(A)-(c), (d)(2), (d)(3).
\(^{103}\) See ibid. (citing Nimmer, at section 12B.07[C] p. 12B-64).
\(^{104}\) DMCA. Section 512(c)(2)
accessible to the public and by providing to the Copyright Office the name, address, phone and
electronic mail of the agent, as well as other contact information which the Register of
Copyrights may deem appropriate. Moreover, the notification of claimed infringement must
be a written form, provided to the agent, that includes substantial elements, such as, a physical
or electronic signature of a person authorized to act on behalf of the owner of an exclusive
right that is allegedly infringed, Identification of the copyright worked claimed to have been
infringed, and Identification of the material that is claimed to be infringing or to be the subject
of infringing activity.

The notice and takedown procedure considers knowledge of ISPs on infringing activities as a
prime matter by establishing statutory law which constitute knowledge of ISPs whether they
have actual knowledge or constructive knowledge (awareness). Hence, ISPs must conform
to the procedure only when they have actual knowledge or awareness of allegedly infringing
activities. In this relation, the first way that ISPs can be put on notice of infringing materials on
their systems is notifications from copyright owners. The notification from copyright owners is
essential since ISPs do not have the ability to gain actual knowledge unless they receive the
notification from copyright owners. As a result, in case that copyright owners fail to comply
with requirements concerning element of notification, it will be considered as no-existent
knowledge of ISPs. Moreover, the DMCA establishes awareness criterion, in which this is the
second way that ISPs can be put on notice that their systems contain infringing materials. In this
regard, awareness criterion intends to express that ISPs have an obligation of monitoring their
systems if they have a special reason to suspect that infringing activities are taking place. This
can best describe as a “red flag test”. The red flag test stems from the language in the statue
that requires ISPs to take action when they become aware of a red flag from which infringing

105 See ibid. Section 512(c)(2)(A)-(B).
107 See ibid. Section 512(c)(1)(A)(i).
108 See ibid. Section 512(c)(1)(A)(ii).
109 See ibid.
110 See ibid. Section 512(c)(3)(B)(i)
111 See supra note 3, K. Koelman, p. 30.
activity is apparent. According to the committee report, the “red flag” test has both a subjective and an objective element. In determining whether the service provider was aware of a “red flag,” the subjective awareness of the service provider of the facts or circumstances in question must be determined. However, in deciding whether those facts or circumstances constitute a “red flag” or in other words, whether infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances, an objective standard should be used.\textsuperscript{113} Moreover, the committee sought to distinguish the red flag test from the mere constructive knowledge, “should have known,” standard typically applied in contributory liability cases. The committee reports specifically provide that the DMCA’s knowledge standard differs from existing law, under which a defendant may be liable for contributory infringement if it knows or should have known that the material was infringing.\textsuperscript{114} In this regard, the reports underscore that the infringements must be apparent “from even a brief and casual viewing.” Reading this legislative history, scholars have concluded that “the ‘flag’ must be brightly red indeed and be waving blatantly in the provider’s face.”\textsuperscript{115}

Furthermore, the DMCA established the protection for ISPs from being held liable for any kind of liability where they take down claimed infringing materials incorrectly on the basis of a good faith.\textsuperscript{116} However, in order for ISPs to be exempted from being held liable for taking down claimed infringing materials, the DMCA states that to have protection from all claims, ISPs who remove the material upon obtaining the notification which are believed to be illegal must promptly notify the subscriber that they have removed or disabled access to the material.\textsuperscript{117} Moreover, ISPs have to put the material back online or cease disabling access to it upon receiving a counter notification from the website owner claiming that the removal was


\textsuperscript{114} \textit{See ibid}, p.25


\textsuperscript{116} DMCA. Section 512(g)(1).

\textsuperscript{117} \textit{See ibid}. Section 512(g)(2)(A)
unjustified. In addition, the counter notification must comply with requirements which are similar to the notification of claimed infringement, but also must contain some sort of choice of forum provision.

3.3.3 Case law

Napster Litigation

The Napster litigation began on 6 December 1999, when A&M Records and 17 other record companies filed a complaint against Napster for contributory and vicarious copyright infringement. The plaintiffs alleged that Napster knew of the infringing activities but failed to prevent its users’ unauthorized reproduction and distribution of the plaintiffs’ copyrighted music. In May 2000, Napster brought a motion for summary judgment relying on the mere conduit safe harbor in section 512(a) of the DMCA. The plaintiffs argued that Napster’s directory and search facilities disqualified it from the mere conduit safe harbor. The plaintiff further claimed that the services of Napster fell within the information location tools safe harbor in section 512(d) and even though section 512(a) applied to the case, the plaintiffs relied on the fact that the music was not transmitted or routed through the Napster system, but directly between it users over the internet. Napster countered that the information location tools it provided were incidental to its main function of transmitting or routing MP3 files for users and that even if they fell within section 512(d), the safe harbor in section 512(a) covered the other aspects of its service. The District court refused to considered Napster as a mere conduit of information and refused to grant section 512(a) safe harbor protection holding

118 See ibid. Section 512(g)(2)(B)-(C).
119 See ibid. Section 512(g)(3)(A)-(D).
120 See summary of the case, B. Mercurio (see supra note 58) and V. McEvedy (see supra note 101, pp.5-6.)
121 Napster is the epitome of what has become known as “peer-to-peer” file sharing. Users may load files onto their own computers and by connecting to the Napster system, allow any other user in any location to retrieve that file on demand. Users can make works available at their own choosing, and can locate and obtain electronic copies of materials that any other person may have chosen to enter into the system. Napster, Inc., the named defendant in this case, does not maintain a central computer system that stores and delivers content files. Instead, individual users employ Napster’s software to find and locate files that are stored on the computers owned by other individuals who connect voluntarily to Napster’s system; see http://www.dml.indiana.edu/pdf/AnalysisOfNapsterDecision.pdf
123 DMCA. Section 512(a)(5).
124 See supra note 112, at 919.
that Napster’s role in transmission of MP3 files did not occur through Napster’s system. That is, Napster allowed users to locate and directly exchange MP3 files by routing the request of a user to another user’s browser instead of transmitting the files through its system. Therefore, the court refused to apply the section 512(a) to Napster’s role. Moreover, the court found that Napster had failed to comply with the general eligibility requirement applicable to all safe harbors in section 512(i) which required that an ISP must adopt, implement and inform its users of a policy for terminating repeat infringers. In February 2001, the Circuit Court of Appeals affirmed the District Court’s findings, holding that Napster had infringed copyright and that neither protection under the DMCA or the fair use doctrine could be applied. The court further ruled that Napster must prevent users from gaining access to copyrighted content available from other users. The decision forced Napster to shut down its operation.

According to Napster, even though the case did not show the victory of an ISP, the case showed how the court considered the safe harbor protection toward an ISP, as well as how court interpreted the coverage of ISP’s definition by ruling that Napster was not a service provider within the meaning of section 512(k)(1)(A) of the DMCA. This leading case raised up the view that the DMCA provides narrow coverage for definition of ISP since it does not establish the matter of Peer-to-Peer file sharing system. It is possibly a loophole of the DMCA in dealing with rapidly growing technology.125

3.3.4 Evaluating the DMCA

3.3.4.1 The DMCA provides treatment for ISPs not to be held liable on the basis of common law principles

125 See infra chapter 5.
As noted above ISPs are immunized from being held liable where the roles of ISPs fall within the safe harbor, and ISPs comply with the conditions set forth in each safe harbor. Firstly, with regard to direct liability of copyright infringement, it is relatively straightforward that the DMCA relieves ISPs from being held directly liable for copyright infringement where ISPs are solely acting as data conduit, transmitting information, as well as routing and providing services. According to the first safe harbor, supposing the DMCA had implemented at the same time that the Frena case was in consideration of the court, Frena would have chosen to follow the DMCA and would have escaped from being strictly held liable on direct infringement which was too rigid and unreasonable. With regard to the first safe harbor, the role of Frena actually would fall within provision 512(a) because it merely provided subscribers a venue for uploading or downloading such materials which were stored in its system on the purpose of only being transmitted upon receiving a request from another user. Hence, Frena would have been exempted from being held directly liable.

Secondly, in the case of vicarious liability, according to case laws, it was not likely to hold vicariously ISPs liable because they required factors for vicarious liability are unable to be fulfilled. Therefore, courts hesitated to hold ISPs liable for vicarious liability in most cases. The DMCA, in this respect, does not make any different from required facts of vicarious liability since the provision 512(c) requires the right to supervise and the financial benefit which are the same factors that courts required. As a result, ISPs in this perspective are less likely to follow DMCA to escape vicarious liability unless courts would expand the existing factors of the ability of supervision and direct beneficial interest from infringements.\(^{126}\)

Thirdly, in the case of contributory liability, the provision 512(c) establishes the notice and takedown procedure which requires knowledge of ISPs on the infringing activities, and provides immunity for ISPs who acts expeditiously responding to a request from copyright owners. ISPs who continue to provide infringing subscribers the internet service will be held liable for contributory liability. In this relation, previously the existing law was not clear as to the degree

\(^{126}\) See supra note 34, A. Yen, p. 50.
of evidence necessary to create constructive knowledge on the part of ISPs that do not actually know of third-party infringement. The DMCA introduced the stringent knowledge standard which is explicit about what can constitute actual knowledge or constructive knowledge (awareness), and therefore it could provide higher protection for ISPs. That is, in the case that the designated agent is informed about infringing activities and when the agent receives the notification containing substantial information set forth according to the Act, then the knowledge of ISPs is in the determination whether they have actual knowledge of infringing activities. In other word, if copyright owner fails to do so, it is not sufficient to assume that ISPs have actual knowledge. Moreover, the DMCA describes awareness criterion, which requires ISPs to take action when they are aware of facts or circumstances in which infringing activity is apparent, on the basis of red flag test. The red flag test constitutes information of any kind that a reasonable person would rely upon in determining that material is infringing. This constructive knowledge standard is more stringent than pre-existing knowledge standard for contributory infringement. Consequently, the DMCA makes it stricter for a plaintiff to prove the knowledge of ISPs.

### 3.3.4.2 No liability for taking down

According to the noticed and takedown procedure, ISPs must respond promptly to take down the allegedly infringing material or disable access to the material that is claimed to be infringing upon receiving the notification of claimed infringement from the copyright owner. In this light, as noted above in the era of Pre-DMCA, ISPs had been in the dilemma since ISPs, on the one hand, had to act in conformity to the procedure immediately upon receiving the notification. On the other hand, they were at risk that they were likely to be sued by person whose material had been taken down when the claimed infringing material turned out to be not infringing at all. In this regard, it might affect ISPs negatively in case they have to remove

---

127 See ibid.
129 According to the previous case law, ISPs will be held liable for contributory infringement if they knew or should have known that the material was infringing
the unproven material or suspend the user to access to the internet since it might be the case that the notification contains errors. The DMCA provides protection for ISPs regarding this issue by stating that there is no liability for taking down generally. In this way, the law protects ISPs when they take down on request of copyright owners on the basis of good faith and they promptly notify a person whose material has been taken down that the claimed infringing material has been removed or disabled access to it. Then they will not be held liable for taking material down.

3.3.4.3 The DMCA provides great certainties for ISPs

The greatest benefit that the DMCA provides to ISPs is legal certainty that keeps ISPs out of the hand of judges. The DMCA prescribes exactly what is expected of ISPs in the fight against copyright infringement, establishes the limitations of liability upon them where their acts fall within the safe harbor, as well as immunizes them when they act as a good citizen by cooperate with copyright owners to combat copyright infringements. Besides, the DMCA establishes the knowledge standard which provides a clear situation for ISPs that in which circumstances they will be assumed to have actual knowledge or constructive knowledge. Moreover, ISPs are provided protection from being held liable where they take down claimed infringing material on the basis of good faith. Finally, the DMCA does not establish the provision that requires ISPs to bear a burden of policing their systems. In this light, the DMCA states that ISPs have no affirmative duty to monitor their services or to affirmatively seek facts indicating infringing activity.

3.3.4.4 The Notice and takedown is a good incentive

---

130 DMCA. Section 512(g)(1).

131 In Rossi v. MPAA, 391 F.3d 1000 (9th Cir. 2004), the Ninth Circuit established that for the purposes of DMCA the “good faith” standard should be subjective and does not require an objective showing of suspected infringement, such as results of a “reasonable investigation”.

132 See ibid. Section 512(g)(2)(A).


134 See supra note 82, C. Beams, p. 845.

135 See ibid.

136 DMCA. Section 512(m).
The DMCA is perceived to be a successful Act to fight online copyright infringement by providing the notice and takedown procedure. The procedure explicitly shows the cooperation between ISPs and copyright owners which both benefit from working together. Copyright owners, of course, have incentives to participate in the procedure since their exclusive rights will be protected and they will gain money to cover their damages. In turn, ISPs, by complying with the procedure, will be shielded from being held liable and can escape from monetary relief. As this procedure is beneficial to both parties, they will obey in order to protect their own interests.

3.4.4.5 Guarantee freedom of expression and fair competition

The DMCA guarantees freedom of expression by giving a person whose material claimed to be infringing an opportunity to protest by submitting a counter notification in order to request to put the material back online or cease disabling access to such material when it has been proved later that the removal or the disablement is unjustified.\footnote{See \textit{ibid.} Section 512(g)(2)(B)-(C).} Moreover, the DMCA deals with unfair competition matter by establishing that any person who knowingly misrepresents that material is infringing or mistakenly removed, is liable for the damages incurred as a result of a service provider acting upon such misrepresentation.\footnote{DMCA. Section 512(f).} In this regard, copyright owners who give false notifications to ISPs will be penalized under the DMCA. This could reduce a number of improper notifications which intentionally are aimed to eliminate competition in business. In addition, copyright owners are deterred from sending improper notifications not only by the provision of the DMCA but also by the prospect of bad publicity and judicial sanction.\footnote{J. Reichman, G. Dinwoodie & P. Samuelson, (2007), ‘A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works’, \textit{Berkeley Technology Law Journal} 981, \textit{UC Berkeley Public Law Research Paper} No. 1007817, \textit{Duke Science, Technology & Innovation Paper} No. 24.}

3.3.5 Conclusion
In summary, the DMCA proved averagely effective as a solution for online copyright infringement cases involving users and their ISPs. The two main purposes of the DMCA have been proved successful. First, regarding the purpose of providing incentives for both ISPs and copyright owners to detect and combat online copyright infringements. In this regard, copyright owners have incentives to monitor internet sites for infringing materials and to provide appropriately detailed information to ISPs so that infringing materials can be taken down. Moreover, copyright owners are prevented from sending false notifications intentionally by the provision of the DMCA that penalizes persons who send improper notifications. In return, ISPs have incentives to cooperate with copyright owners by complying with the notice and takedown procedure otherwise they will lose the safe harbor protection provided by the DMCA. Second, regarding the purpose of providing legal certainty for ISPs, the DMCA accomplished three main objectives 1) codified into statutory law that passive automatic acts cannot be a foundation for finding of online copyright infringement; 2) made it harder to establish a case of contributory or vicarious copyright infringement against ISPs; and 3) in cases where an ISPs take action against alleged copyright violators, protected ISPs from lawsuits when they act to aid copyright owners in restricting or impeding infringements. In this light, the DMCA not only allows ISPs to be secure as to what exactly the law is, but also reaches a fair conclusion as to what that standard should be.

In this chapter, it is clear that before the enactment of the DMCA, the US has dealt with the issue of ISP liability by applying judge-made copyright legal doctrines which are not justifiable. According to the Pre-DMCA era, it seemed that it was not sensible for ISPs to be held liable merely they acted as passive conduit, to be responsible of monitoring their systems, to be liable for third-party copyright infringement without knowledge, or to be responsible for liability which may arise when they took down allegedly infringing materials on the basis of good faith.

141 See supra note 139, J. Reichman, G. Dinwoodie & P. Samuelson, p. 24
142 See ibid.
144 See supra note 82, C. Beams, p. 841.
The DMCA, at present, seems to be a right solution to secure ISPs from being held liable for direct infringement when an act of ISP as merely a data conduit. Furthermore, the DMCA establishes the knowledge standard which is clear to ISPs that what constitute sufficient knowledge in contributory liability. Moreover, the safe harbor makes it clear for the extent of liability by establishing protection for ISPs who perform certain activities according to the Act. Moreover, the notice and takedown procedure not only provides an opportunity for ISPs to cooperate with copyright owners in order to be immunized, but also provides protection for ISPs not to be held liable for any liability which may arise in relation to takedown procedure.

However, there are contrary comments, which are not the prevailing view, on this legislation. One commentator can rarely see the point in this legislation, rather thinks that it is better to wait and see how the case law develops itself.\textsuperscript{145} Another one supports that perspective stating that this legislation is not necessary because “courts had not yet interpreted copyright law in a manner which would have a chilling effect on ISPs, and legislation constrains the courts at the very time they need the most room to develop ISP liability doctrines”.\textsuperscript{146} However, as abovementioned, the DMCA was added in the existing law, meaning that the good old law and judge-made principles remain intact. Therefore, it is not always the case that ISPs will be shielded from direct liability where they perform activity which falls within the first safe harbor. For example, the Frena case is still a good law remaining open in other jurisdictions and could be followed by a future court.\textsuperscript{147}

\textbf{Chapter 4}

\textbf{EU Approach: E-Commerce Directive 2000}

\textsuperscript{145} See supra note 2, H. Salow, p. 48 (citing On-Line Copyright Liability Limitation Act and WIPO Copyright Treaties Implementation Act: Hearing on H.R. 2280 and H.R. 2281 before the subcommittee on courts and Intellectual Property of the house Judiciary Committee (statement of Michael K. Kirk, Executive Director AIPLA)).


\textsuperscript{147} See supra note 34, A. Yen, pp. 49-50.
4.1 Introduction

Similarly to the US, the EU has become aware of the issue of ISP liability. Before an enactment of the ECD, each Member State had its own legislation governing copyright infringement and some Member States already had specific regulations on ISP liability.\(^{148}\) Those countries that did not have specific legislation on ISP liability had regulated this issue through case law.\(^ {149}\) Moreover, in countries where there was no case law, the liability of online intermediaries was dealt with by applying general laws governing tort liability and specific law for copyright.\(^ {150}\) Unlike the US regulation described in the previous chapter, this chapter is not going to deal with kinds of liability applying to ISPs before the enactment of the E-Commerce Directive (hereinafter ECD)\(^ {151}\) since each Member State had its own national law and therefore the statutory rule on ISP liability differed from one country to another. However, basically, types of liability that were applicable to ISPs are strict liability and secondary liability which have been adopted from tort law\(^ {152}\), and again it differed from one jurisdiction to another. The ECD aimed to be the leading law that each Member State has to impose upon its own national legislation. However, even if there is common regulation, the way Member States implemented into their own laws is different. This chapter will particularly deal with the ECD which contains specific rules on ISP liability. The first paragraph will shortly explain the background and the main purpose of the ECD. The next paragraph will describe section 4 of the ECD which contains the matter of liability of intermediary service providers. After that, case law and an analysis of the ECD will be provided respectively.

4.2 E-Commerce Directive 2000

To make it clear from the start, the purpose of the ECD is not focused solely on copyright infringements. The main reason behind the enactment of the ECD is to contribute to the proper functioning of the internal market by ensuring the free movement of information society

\(^{148}\) For example Germany has Multimedia Law which addressed the scope of liability of on-line service providers, and Sweden has a law regarding responsibility for electronic bulletin board which appears to be applicable to other on-line intermediaries. See R. Julia-Barcelo, (1999), 'Liability for On-line Intermediaries: A European Perspective', intellectual property review, pp. 8-11.

\(^{149}\) See ibid, R. Julia-Barcelo, pp.11-13.

\(^{150}\) See ibid, pp.13-14.

\(^{151}\) Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Marker, passed 8 June 2000.

\(^{152}\) See supra note 3, K. Koelman, pp.8-11.
services between the Member States. That is, the main purpose of the ECD is to enhance e-commerce among Member States. Before the enactment of the ECD, the growth of e-commerce had been rapid, by the year 2000, its worth exceeded 17 billion euro and it was expected to reach 340 billion euro by the end of 2003. In order to respond to the growth of e-commerce, the European Commission needed to harmonize the law among Member States. The uniformity of the law and the coordination among Member States will enhance the development of information society services, ensure legal certainty and build up consumer confidence. The original proposal for the ECD considered five crucial issues; (1) establishment of Information Society service providers; (2) commercial communications; (3) online conclusion of contracts; (4) liability of intermediaries; and (5) implementation. The issue of ISP liability is significant because it is relevant to the development of cross-border services among Member States. With regard to recital 40 of the ECD, it is noted that “both existing and emerging disparities in Member State’s legislation and case law concerning liability of service providers acting as intermediaries prevent the functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition”. The ECD then was enacted aiming to solve these internal market problems by introducing safe harbors for certain types of intermediary. In addition, the enactment of the ECD was aimed to bring the law into international level which responds to the enforcement of WIPO Copyright Treaty. In particular, the ECD deals with the liability of intermediaries throughout Europe. The regime is very widely drawn, effecting not just ISPs, but “ISSPs”: “information society service providers” or, as the title of Section 4 of the ECD also calls them “intermediary service providers”. An “information society service” is defined as “any service

153 ECD, Art. 1(1).
156 ECD, Recital 40.
158 See supra note 66.
159 ECD, Art.2 (b). These providers can be natural or juristic person.
normally provided for remuneration, at a distance by electronic means and at the individual request of a recipient of services". According to the definition, it was broadly drafted; the intermediary service provider liability regime covers not only the traditional ISP sector, but also a much wider range of actors who are involve in selling goods or services online. The ECD takes a horizontal approach to deal with ISP liability, meaning that one liability regime is applicable to any infringements initiated by third parties in the online environment regardless of the area of law. Hence, liability of ISPs according to the ECD covers not only copyright infringement but also the area of defamation, criminal obscenity libel, privacy etc. Moreover, as regards the types of liability covered by the ECD, it should be noted that the ECD applies both to civil and criminal liability for copyright infringement.

4.3 Liability of intermediary service providers
The set of rules regarding ISP liability is laid down in articles 12-15 of the ECD. The rules mainly concern activities of ISPs which can be exempted from being held liable. In this way, in the case that ISPs provide a specific service and comply with a series of requirements, they will be shielded from being held liable. Moreover the limitations of liability apply only to monetary damages, meaning that the ECD do not affect the grant of different kinds of injunction in accordance of national law, meaning that Member States can impose all types of injunction upon online intermediaries. In other word, the ECD does not provide complete protective mantle for ISPs. In particular, the ECD covers three categories of online intermediary functions which will be described in the following section.

160 Article 2(a) of the ECD refers back to the definition in Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC. The definition is discussed further in recital 17 and 18 of ECD.
161 See further supra note 133 L. Edward, pp. 11-13.
162 See supra note 19, P. Basicrocchi, p. 117. See ibid. pp.4-6.
163 See supra note 133, L. Edwards, p.23
165 See supra note 19, P. Basicrocchi, pp. 117-118
166 ECD. Recital 45.
167 See supra note 164, R. Julia-Barcelo & K Koelman, p.231.
4.3.1 Mere conduit

Article 12 provides two types of mere conduit activity. The first consists of “the transmission in a communication network of information provided by a recipient of the service and the second consists of the “provision of access to a communication network”. The former is relevant to the act of ISPs as mere conduit of materials that are provided by third parties, by allowing such materials to be transmitted through their networks. The latter immunizes ISPs from being held liable for providing the internet network. Moreover, the act of transmission and provision of access mentioned above includes the automatic, intermediate and transient storage of the information. This further explains the scope of transmission and access. That is, information is transmitted in a network by being carried from one computer to another computer. Information then is temporally stored for a short period of time on any of these computers, and this temporal storage is also seen as transmission. Moreover, such transmission must take place for the sole purpose of carrying out the transmission in the communication network, and the information must not be stored for any period longer than the certain period that is reasonably necessary for transmission. However, when ISPs meet the conditions that they only act as mere conduit, there will be no liability for ISPs as long as they do not initiate the transmission themselves, do not select the receiver of the transmission and do not select or modify the information contained in the transmission, except for manipulation of technical nature enabling the transmission of the information.  

4.3.2 Caching

Article 13 establishes a limitation of liability for ISPs in case information is automatically, intermediately and temporally stored in their networks for the sole purpose of making more efficient the information’s onward transmission to other recipients of the service upon their  

---

169 ECD, Art. 12(1).
170 See supra note 19, P. Basicrocchi, p. 119.
171 ECD, Art. 12(2).
173 See supra note 19, P. Basicrocchi, p. 119.
174 ECD, Art. 12(1)(a).
175 See ibid, Art. 12(1)(b).
176 See ibid, Art. 12(1)(c).
177 See ibid. Recital 43.
requests.\textsuperscript{178} This automatic, intermediate and temporary storage of data is called caching. The purpose of caching is to decrease the repetitive high demand of certain materials by locating the high demand materials on remote servers, then storing copies of those materials on local servers. In this way, it allows materials to be delivered to users who are seeking for those materials in the quickest way since the data has less distance to travel.\textsuperscript{179} However, ISPs are not liable when they perform caching activities under the conditions that; (1) they do not modify the information,\textsuperscript{180} because then they cannot be considered as intermediaries; (2) they comply with conditions on access to the information,\textsuperscript{181} this condition is relevant because sometime a person who puts the information on the network applies certain conditions to make access available such as payment of fees. ISPs must guarantee that access to cache copies is allowed only in case users comply with access requirements;\textsuperscript{182} (3) they do not interfere with rules regarding the updating of information, specified in a manner widely recognized and used by industry.\textsuperscript{183} In this regard, ISPs must allow information to be updated, especially in the case of information in need of frequent updates such as personal information, scientific or economic information;\textsuperscript{184} (4) they do not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information;\textsuperscript{185} and (5) They must act expeditiously to remove or to disable access to the information stored on their networks upon obtaining actual knowledge that the initial source of the transmission has been removed from the network, or access to it has been disabled, or court or administrative authority has ordered such removal or disablement.\textsuperscript{186} It means that ISPs should ensure that the information they provide is as accurate as possible. Therefore, upon receiving the notification that the

\begin{itemize}
  \item \textsuperscript{178} See ibid, Art. 13(1).
  \item \textsuperscript{179} See supra note 19, P. Basicrocchi, p. 120.
  \item \textsuperscript{180} ECD, Art. 13(1)(a).
  \item \textsuperscript{181} See ibid, Art. 13(1)(b).
  \item \textsuperscript{183} ECD, Art. 13(1)(c).
  \item \textsuperscript{184} See supra note 19, P. Basicrocchi, p. 121.
  \item \textsuperscript{185} ECD, Art. 13(1)(d).
  \item \textsuperscript{186} See ibid, Art. 13(1)(e).
\end{itemize}
information is inaccurate they must remove it from the network or disable access to it promptly.\textsuperscript{187}

### 4.3.3 Hosting

Article 14 establishes a limitation of liability for ISPs where they provide storage space on web servers to third party users. This activity of ISPs is known as hosting.\textsuperscript{188} Therefore hosting defines the service that ISPs offer to individuals, companies, and organizations to rent space and incorporate any kind of data on the space.\textsuperscript{189} According to article 14, ISPs will not be held liable for the third party’s information stored on their servers\textsuperscript{190} under the conditions that; (1) they do not have actual knowledge of illegal activities or infringing information;\textsuperscript{191} (2) they may not be aware of facts or circumstances from which the illegal activity or information is apparent, otherwise they are liable for claim and damages.\textsuperscript{192} According to those conditions, they are differentiated between civil and criminal liability. The former establishes standard for criminal liability, meaning that, ISPs will not be held liable under criminal law for hosting infringing third party’s information unless they have actual knowledge of unlawful activities or infringing information.\textsuperscript{193} It is therefore apparent that ISPs will not be held criminally liable if they have merely constructive knowledge. The latter is not relevant to criminal liability, but instead concerns civil liability for damages. Under this condition, ISPs will not be held liable unless they are aware of facts or circumstances of infringing information or unlawful activities. Hence, the standard to hold ISPs liable for civil liability is constructive knowledge.\textsuperscript{194} However, even if ISPs have actual knowledge or constructive knowledge of infringing information or unlawful activities, they still can be exempted from being held liable when they immediately remove the infringing information or disable access to it upon obtaining such knowledge or

\begin{footnotesize}
\begin{enumerate}
\item \textit{See supra} note 155, A.R. Lodder & H.W.K. Kaspersen, p.88.
\item \textit{See supra} note 183, R. Julia-\textit{Barcelo}, p. 13.
\item \textit{See supra} note 19, P. Basicrocchi, p. 122.
\item ECD, Art. 14(1)
\item \textit{See ibid.} Art. 14(1)(a)
\item \textit{See ibid.}
\item \textit{See supra} note 183, R. Julia-\textit{Barcelo}, p. 13.
\item \textit{See ibid.}
\end{enumerate}
\end{footnotesize}
Moreover, it further states that the conditions mentioned above will not be applied when the recipient is acting under the authority or the control of the ISP.196

4.3.4. No general obligation to monitor

Article 15 states that ISPs who provide services which fall within article 12, 13 and 14 will not be imposed a general obligation to monitor the information they transmit or store. Moreover, a general obligation to actively seek facts or circumstances indicating illegal activity does not exist either.197 Although the ECD prohibits Member States to impose a general obligation of monitoring upon ISPs, it does not mean that ISPs do not have a monitoring obligation in a specific case.198 Moreover, in order to detect and prevent certain types of illegal activity, ISPs will be imposed a duty of care which can reasonably be expected from them and which are specified by national law.199 However, article 15(2) establishes two specific obligations for ISPs. First, by requiring ISPs to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipient of their service as soon as ISPs become aware of it, and second, to disclose the identity of recipients with whom they have a storage agreement upon receiving a request from competent authorities.

4.4 Case law

195 ECD, Art. 14(1)(b).
196 See ibid, Art. 14(2).
197 See ibid. Art. 15(1).
198 See ibid. Recital 47. It states that in a specific case, article 15 does not affect orders by national authorities in accordance with national legislation.
199 See ibid, Recital 48.
**Sabam v. Tiscali (Scarlet)**

The recent Belgian decision in SABAM v. Tiscali (Scarlet) appears to be the first time in Europe a court has considered whether ISPs can be required to monitor or filter the activities of their users in order to stop file sharing on Peer to Peer networks (hereinafter P2P). The Court of First Instance in Bruxelles has ordered Scarlet, a Belgium ISP, to implement technical measures in order to prohibit its users to illegally download music files. The decision came after a complaint initiated in 2004 by Sabam (Belgian Society of Authors, Composers and Publishers) against the Belgium ISP Tiscali, now renamed as Scarlet. A first intermediary ruling of 26 November 2004 accepted the possibility for an ISP to disconnect customers if they violate copyrights, and block the access for all customers to websites offering file-sharing programs. The court has decided that Scarlet need now to implement one or more technical measures in order to stop the copyright infringement, by making it impossible for its subscribers to send or receive music files from the repertoire of Sabam via P2P software. Scarlet also needs to inform Sabam on the technical measures that will be implemented. The decision needs to be implemented in 6 months, or the ISP must pay 2500 euro/day as damages for non-compliance.

The decision did not consider the issues regarding privacy, freedom of expression or the right to the secrecy of the correspondence. Scarlet also claimed that the duty imposed by the court is a general obligation to monitor the network that is contrary to article 15 of the ECD. But the court ruled that because the technical measures are limited to the blocking or filtering of only certain information transmitted on Scarlet's network, it did not constitute a general duty to monitor.

Scarlet also argued that the installation of filtering measures may lead to the loss of the safe harbor from liability for mere conduit activities that technical intermediaries enjoy by virtue of article 12 of the ECD. In this relation, Scarlet wrongfully considers that this injunction would

---

result in its loss of the safe harbor from liability since in accordance with recital 45, the ECD establishes that “the limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by court . . . requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it.” Therefore, the court had possibility to order the injunction which required Scarlet to apply filtering measure.

This decision was met with great satisfaction by international rights holders groups, such as the International Federation of Phonographic Industries (IFPI), which issued a press release stating: "this is an extremely significant ruling which bears out exactly what we have been saying for the last two years that the Internet's gate-keepers, the ISPs, have a responsibility to help control copyright-infringing traffic on their networks. The court has confirmed that the ISPs have both a legal responsibility and the technical means to tackle piracy."

Nevertheless, the court decision raised several serious concerns. Not only did the court seem to apply questionable logic that the use of filtering technology does not constitute a general obligation of monitoring, but also the ruling seemed to also stand in conflict with Article 12 of the ECD, which grants immunity to ISPs when they serve as mere conduits. Furthermore, there is doubtful whether the court's ruling means that Scarlet has a legal duty to implement technical measures against illegal file sharing. If so, as it appears, then all ISPs operating in Belgium would have the same duty. And if that is the case, then internet users in Belgium could not simply switch ISPs to avoid filtering, as no ISPs could operate in that country without deploying one of the measures set forth in the expert's report. There is also the precedential impact of the ruling that if mandated content filtering can be interpreted by one court as lawfully consistent with articles 12 and 15 of the ECD, then other courts may find it easier to

---

reach the same conclusion.\textsuperscript{203} Indeed, as expressed by IFPI CEO John Kennedy, "this is a decision that we hope will set the mold for government policy and for courts in other countries in Europe and around the world."\textsuperscript{204} However; even though the ruling could influence courts in other EU member states, it will have been based on the particular Belgian laws which implemented the ECD, and so its impact could be limited.

### 4.5 Evaluating the E-Commerce Directive

#### 4.5.1 The ECD harmonizes the laws among Member States

Before the enactment of the ECD which requires Member States to impose the directive into their national legislations, as noted above, Member States have addressed the issue of ISPs liability in different ways according to their national laws. Some of them addressed this problem by introducing new regulation specifically aimed at ISP liability,\textsuperscript{205} while those which did not have specific legislation to govern ISP liability relied on case law or general tort law.\textsuperscript{206}

The different principles of coping with liability of intermediaries among Member States could be the source of obstacles of the development of the internal market. In other words, national legislation or case law which is different from one country to another country impairs the development of cross-border services. Therefore, the ECD is introduced as a guideline legislation which could unify the pattern of legislation concerning ISP liability. Nevertheless, Member States have implemented the ECD in their national laws differently. As the case demonstrated above, Belgium implemented the ECD into its law which required ISPs to employ technologies to monitor their systems, while other countries might find it is too burdensome to impose a monitoring obligation upon ISPs. This depends on national law because the ECD does not affect the authority of national law and leaves room for Member States to apply the law in a suitable ways. This might raise the issue that the ECD does not do well to protect ISPs from being imposed a burdensome obligation. According to recital 47, as long as the ECD does not affect orders by national authorities in accordance with national legislation, ISPs still seem to be

\textsuperscript{203} See ibid.

\textsuperscript{204} IFPI, IFPI hails court ruling that ISPs must stop copyright piracy, July 4, 2007, \url{www.ifpi.org/content/section_news/20070704b.html}, last visited on 18 July 2009.

\textsuperscript{205} See supra note 148.

\textsuperscript{206} See supra note 149.
in a vulnerable situation. Furthermore, recital 48 emphasizes that the ECD does not affect the possibility of Member States of requiring ISPs to apply a duty of care. This recital is obviously in contradiction to article 15 which states that ISPs will not be imposed a general obligation of monitoring their systems. It remains to be seen how these provisions can be reconciled.\footnote{See supra note 164, R. Julia-Barcelo & K Koelman, pp. 232.}

### 4.5.2 The ECD provides certainties for ISPs

The ECD was developed in the same vein as the DMCA. Apart from the main purpose of the ECD that it aims to eliminate existing legal uncertainties and to avoid divergent approaches at Member State level in order to encourage confidence in the single market\footnote{J. Soma & N. Norman, (2000), ‘International Take-Down Policy: A Proposal for WTO and WIPO to Establish International Copyright Procedural Guidelines for Internet Service Providers’, Hastings Communications and Entertainment Law Journal, Vol. 22, No. 391, p. 13.}, the provisions on the limitations of intermediaries provide certainties for ISPs in the same manner as the DMCA. In this light, the ECD focuses on simplifying behavioral, procedural standards in order to clarify the responsibility of ISPs for transmitting and storing materials at the request of third parties.\footnote{See ibid.}

The ECD seeks to relieve the fear that content owners will lose the value of their works and that ISPs could face potentially unlimited liability for content passing through or stored on their networks by subscribers\footnote{See ibid.} by introducing the safe harbor for certain types of intermediaries. ISPs can be secured in case their activities fall within safe harbors and they conform to the conditions set forth according to the ECD. Furthermore, the important thing which is fundamental for ISPs is that they have no general obligation of monitoring their networks.

### 4.5.3 No notice and takedown procedure

\footnote{See supra note 164, R. Julia-Barcelo & K Koelman, pp. 232.}
4.5.3.1 Uncertainty for ISPs

The ECD does not establish the notice and takedown procedure as the DMCA explicitly does. Nevertheless for the hosting activity, the ECD requires ISPs to comply with the conditions in order to be shielded from being held liable. According to article 14, if ISPs have actual knowledge or have awareness of infringing materials, and expeditiously remove allegedly infringing materials or disable access to such materials, ISPs will not be held liable. This procedure seems to be identical to the notice and take down procedure of the DMCA, but it is somewhat different. First, the ECD does not establish the protection for ISPs in case they take down the claimed allegedly infringing material incorrectly on the basis of good faith. In this relation, ISPs might face a dilemma since they have to respond immediately to the notification of claimed infringement in order to be exempted from being held liable, while at the same time the take down procedure might lead ISPs to be sued if they take down the material which they reasonably believe to be infringing material but it is later proved not to be infringing. Therefore, it results in an insecure situation for ISPs that they might be sued for taking down claimed infringing material incorrectly on the basis of good faith.

4.5.3.2 Freedom of expression

The ECD seems to disregard the matter of freedom of expression. It does not give persons whose materials have been taken down an opportunity to object to the take down nor initiate the process to put materials back online, where the notification of claimed infringement is later proved incorrect, and therefore freedom of expression is severely hindered.211

4.5.3.3 ISPs act as a censorship body

As noted above, ISPs seem to be very cautious and remove claimed infringing material even if it is doubtful that it actually violates someone’s right. Hence, freedom of expression will be controlled by ISPs who promptly shut down or eliminate infringing materials anytime in order to avoid being held liable.212 This might too much rely on ISPs to decide what should be

---

212 See supra note 183, R. Julia-Barcelo, p. 15.
kept or removed, and therefore may cause ISPs to become a sort of censorship body.\textsuperscript{213} There are sensible reasons why it should not be up to ISPs to determine whether certain materials should be removed. ISPs are not well-equipped to deal with such issues because; first, ISPs as technical intermediaries are not at all like publishers. Unlike publishers, ISPs do not have knowledge of the source and the content of allegedly infringing material. Moreover, ISPs mainly deal with the provision of technical facilities for the dissemination of content, while the business of a publisher is directly related to the content of published materials; second, ISPs do not have skills, knowledge or personnel to evaluate whether certain material transmitted through their services is infringing. Therefore, ISPs is not in the right place to judge whether claimed infringing material should remain open to public because they have neither obligation nor ability to do so.\textsuperscript{214}

\textbf{4.5.3.4 Unfair competition}

As abovementioned, ISPs seem to take down claimed infringing material as quick as possible upon obtaining notification which may not only be based on a good faith, but mistaken belief that one’s rights are infringed.\textsuperscript{215} This might resulted in an unfair competition since it encourages parties to give notices and demand takedowns to eliminate competition.\textsuperscript{216} Furthermore, it is apparent that the ECD lacks a statutory provision that can constitute liability to one who intentionally gives fault or incorrect notifications to ISPs.

\textbf{4.5.4 No knowledge standard}

In this regard, the ECD does not establish a particular statute that will be applied in the determination whether ISPs have knowledge or awareness of infringing activity. That is, it is not clear as to what constitutes an adequate notice to provide ISPs with the required level of knowledge.\textsuperscript{217} According to article 14, ISPs must act expeditiously to remove infringing material or disable access to it when they have actual knowledge or awareness. It seems difficult to

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{213} See supra note 19, P. Basicrocchi, p. 130.
\item \textsuperscript{214} See supra note 164, R. Julia-Barcelo & K Koelman, pp. 234-234
\item \textsuperscript{215} See supra note 164, R. Julia-Barcelo & K Koelman, p. 234.
\item \textsuperscript{216} See supra note 183, R. Julia-Barcelo, p. 16.
\item \textsuperscript{217} See supra note 183, R. Julia-Barcelo, p. 15.
\end{itemize}
\end{footnotesize}
judge whether a notification of allegedly illegal material is adequate to trigger the required level of knowledge. Hence, it is difficult to determine adequate knowledge in article 14 which requires two levels of knowledge; actual knowledge is required in case to hold ISPs criminally liable and constructive knowledge is required to hold ISPs liable in the area of civil law. Lacking of a statutory of knowledge standard, the ECD will have difficulty to judge whether ISPs can be held liable.

4.6 Conclusion
The ECD has answered the question that to what extent ISPs should be responsible for online copyright infringement by establishing a set of rules concerning the limitations of intermediary liability in articles 12-15. The ECD provides the protection for ISPs who perform certain activities and comply with the conditions set forth in the ECD. Moreover, the ECD harmonized the laws among Member States, and therefore it can enhance the development of the internal market. However, Member States apply the ECD to their national legislation differently. Moreover The ECD does not affect the possibility for Member States to deal with ISP liability issue in accordance with their national laws, meaning that national legislations remain intact. Nevertheless, the ECD falls shot in some areas. The main areas that the ECD does not cover are that it does not provide protection for information location tool providers. Hence, in this regard it depends on the national law of each Member State whether ISPs are liable where they provide information location tool services. Moreover, the ECD does not establish the notice and take down regime, and therefore problems arise regarding the knowledge standard, freedom of expression and unfair competition as explained above.

Chapter 5
Analysis of the regulatory frameworks

---

218 See ibid.
219 See ibid.
5.1 Introduction

To this point, the thesis has been processed in a way to address the research question and sub-questions that different regimes codified the issue of ISP liability into their statutory laws which generally provide legal certainty for ISPs. Moreover, the two previous chapters obviously explained benefits of the enactment of both legislations that both legislations provide solutions for unlimited potential liability imposed upon ISPs. That is, basically, both regulations establish certain functions of ISPs that can be immunized from being held liable. Furthermore, both legislations require ISPs to comply with requirements set forth in the legislations in order to take advantage of the limitations of liability. This chapter will do a comparison between both regulatory frameworks, and point out some loopholes of both legislations.

5.2 Comparison of the legislations

5.2.1 Definition of ISP and purpose of legislations

The DMCA defined ISPs as either “an entity offering transmission, routing, or providing connections for digital online communication, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the material as sent or received” or, more widely, “a provider of online services or network access, or the operator of facilities thereof”. The first definition covers the function of ISPs as a passive conduit which responds to the first safe harbor while another definition is broader which responds to the another three safe harbors. The broader definition appears to cover traditional ISPs, search engines, bulletin board system operators and even auction web sites. However, US courts have refused to extend these safe harbor provisions to Napster software programs and to similar systems. As discussed above, Napster had not been protected by the safe harbor

---

220 DMCA, section 512(k)(1)(A).
221 See ibid. section 512(k)(1)(B).
223 See supra note 133, L. Edwards, p.11.
224 According to Napster case, court ruled that Napster operation did not fall within section 512(a) because Napster’s role in transmission of MP3 files did not occur through Napster’s system. That is, Napster allowed users to locate and directly exchange MP3 files by routing the request of a user to another user’s browser instead of transmitting the files through its system.
since the operation of Napster fell outside the coverage of ISP’s definition. In this relation, the controversial issue was whether Napster is qualified to be immunized under the safe harbor. This left open the question of whether P2P networks can ever qualify for the safe harbor protection.225

The ECD deals with the liability of intermediaries throughout Europe. The regime is very widely drawn, effecting not just ISPs, but “ISSPs”: “information society service providers”226 or, as the title of section 4 of the ECD also calls them “intermediary service providers”. An “information society service” is defined as “any service normally provided for remuneration, at a distance by electronic means and at the individual request of a recipient of services”.227 According to the definition, it was broadly drafted; the ECD intermediary service provider liability regime covers not only the traditional ISP sector, but also a much wider range of actors who involve in selling goods or services online (eg, e-commerce sites such as Amazon and Ebay); offering online location information or search tools (eg, Google, MSN or LexisNexis); and pure telecommunications cable and mobile communication companies providing access services.228 However, according to the term “at the individual request of recipient”, it excluded TV and radio broadcast form the ECD liability regime since those providers provide service routinely, even if there is no demand from recipient.229

The purpose of the DMCA is to provide incentives for both ISPs and copyright owners to cooperate with each other in order to combat copyright infringement incurred through the digital networked environment and, in the same time, provide legal certainty for ISPs. The ECD similarly concerns about these issues by establishing provisions regarding certain functions of ISPs which fall within the limitations of liability. However, the ECD does not purely focus on

225 See ibid.
226 ECD, Art.2 (b). These providers can be natural or juristic person.
227 Article 2(a) of the ECD refers back to the definition in Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC. The definition is discussed further in recital 17 and 18 of ECD.
229 See ibid.
providing legal certainty for ISPs with regard to copyright infringement, but also aims to eliminate disparities among Member States concerning the matter of ISPs, which might impede cross-border services, by harmonizing laws among Member States.

5.2.2 Vertical approach and horizontal approach

There are two approaches to deal with the liability of ISPs. The crucial difference between the two approaches is the scope of application. In a vertical approach, different liability regimes apply to different area of law. The DMCA adopted this approach, meaning that the DMCA was codified in the existing law, the Copyright Act of 1976; it therefore applies merely to copyright issues whereas the Communications Decency Act of 1996 which is part of the Telecommunications Act provides a broad exemption from liability of online intermediaries for infringement of any type of law other than copyright. On the other hand, the ECD intends to set limits upon civil as well as criminal liability in horizontal approach. In other words, it applies a single liability standard to any infringing issues whether intellectual property, criminal obscenity, libel etc., regardless of area of law. The horizontal approach has an obvious advantage of providing a measure of legal security to ISPs and injured parties across the board to all area of law involving ISPs. This creates uniformity to determine the extent of ISP liability in Europe and avoids an uncertainty of having a different standard concerning a determination when ISPs face potential liability among Member States. However, it is argued that a horizontal approach is favorable since the copyright law has certain unique characteristics that require a different legal and technological treatment. Hence, the threshold will be set too low,

230 B. Hugenholtz, (1999), ‘Online Service Provider Liability for Copyright Infringement’, WIPO workshop on service provider liability, p. 34.
231 See supra note 19, P. Basicrocchi, p. 117.
232 See supra note 137, R. Julia-Barcelo, p. 16.
233 See ibid, p.15.
234 See supra note 183, R. Julia-Barcelo, p. 8
if uniform the liability regime is imposed upon ISPs for third-party copyright infringement of any type of substantive law.\textsuperscript{236}

5.2.3 The Safe harbor

It is apparent that the ECD closely resembles the DMCA in that both of them provide limitations of liability for certain functions performed by ISPs. Firstly, both regulations establish an exemption from liability for ISPs where they play a passive role as a mere conduit of transmitting information. According to The DMCA a function of ISPs as a data conduit of transmitting of online information\textsuperscript{237} resembles a function of mere conduit according to the ECD. A key purpose of this function is that ISPs will not be held liable for the act as a mere conduit of information under the conditions that ISPs do not modify the content, select the receiver or initiate the transmission by themselves.\textsuperscript{238} These conditions, which require ISPs to comply with, are mostly identical between both legislations.

Secondly, caching activity is a certain function of ISPs that falls within the safe harbor. In both legislations, ISPs will not be held liable for performing caching activity that allows information to be stored in transient period of time under conditions that ISPs allow information to be stored in their systems only on the purpose of awaiting to be transmitted by a request of users and may not be maintained for a period longer than a reasonably necessary period for the transmission.\textsuperscript{239} Moreover, to escape from liability for maintaining cache-copies, ISPs must comply with stringent rules established in both legislations.\textsuperscript{240} According to the conditions, both regimes require generally the same conditions that ISPs do not modify the information, ISPs must comply with the conditions on access to information set by content providers; ISPs have to conform to the technology used by the content providers. However, in the last condition which requires ISPs to respond immediately to remove infringing information or disable access to such information upon gaining actual knowledge or awareness, is different. That is, the

---

\textsuperscript{236} See ibid
\textsuperscript{237} DMCA. Section 512(a) and ECD. Art. 12(1)
\textsuperscript{238} DMCA. Section 512(a)(1)-(5) and ECD Art. 12(1)(a)-(c).
\textsuperscript{239} DMCA. Section 512(b)(1)(A)-(C) and ECD. Article 13(1).
\textsuperscript{240} DMCA. Section 512(b)(2)(A)-(E) and ECD. Article 13(1)(a)-(e)
DMCA requires knowledge of infringing activity or awareness of such activity. On the other hand, according to the ECD, required knowledge is not knowledge of infringing activity as such, but knowledge of removal at the initial source or access to infringing material has been disabled, or of the fact that a competent authority has ordered such removal or disablement. Therefore, required knowledge of ISPs under the DMCA is harder to prove which make it more secure for ISPs from being held liable.

Thirdly, ISPs will not be held liable for performing hosting activity. Both legislations establish exemption for ISPs who store information on behalf of third parties under the conditions that ISPs have expeditiously remove claimed infringing material or block access to it when they have actual knowledge of unlawful activity, or they have awareness of facts or circumstances from which infringing activity is apparent. In this regard, the ECD does not provide any guidance on the exact meaning of awareness, but the DMCA does by referring to the red flag test. Moreover, with regard to the conditions, DMCA provides a higher protection concerning vicarious liability by requiring two facts that have to be met. That is, ISP may not receive financial benefit directly attribute to the infringing activity in case in which ISPs have the right and the ability to control such activity, whereas the ECD states that ISPs will not be immunized if the infringing activity done by another is under the authority or the control of ISPs. In this regard, the ECD does not mention about the beneficial interest which ISPs may obtain from infringing activity, meaning that it does not matter whether ISPs gain benefit from infringing activity as long as the infringing activity is done under the authority or the control of ISPs, ISPs will not be limited from being liable.

Finally, it is surprising that the ECD does not provide protection for information location tool providers. Obviously, the ECD does not established the provision concerning the function of ISPs of providing any kinds of referral that can link users to another page, such as search

241 DMCA. Section 512(b)(2)(E).
242 ECD. Art.13(1)(e).
243 DMCA. Section 512(c) and ECD. Article 14.
244 DMCA. Section 512(c)(A)(i)-(iii) and ECD. Article 14(1)(b).
245 See supra note 3, K. Koelman, p. 30.
engines, index or references. Contrary to the DMCA, it establishes that ISPs will not be held liable for providing hyperlinks that lead users to the page which contains infringing materials. The information location tool service is very important in the era of digital networks. For instance, search engines which play a role to allow internet users to find sources, materials, data or any information have become an important tool for internet users. The question which has been raised is whether it is reasonable to impose liability upon ISPs who provide links that can lead to another page containing infringing material. The DMCA has addressed this question by establishing the protection for information location tool providers. The ECD, on the other hand, does not provide the protection for Information location tool providers and it therefore might result in hesitation when a company wishes to do its business in EU countries. According to article 14 of the ECD, it requires undefined word storage which seems to imply that only making a hyperlink to a material cannot constitute hosting, and therefore any liability which may arise in relation to hyperlinks under the ECD will not be excluded by article 14.\textsuperscript{246} In other words, ISPs who provide hyperlinks are not provided immunity. However, European Commission is instructed to review this matter of the ECD on the basis of article 21(2), meaning that the European Commission can re-evaluate the importance of including a liability limitation for ISPs providing these linking services.\textsuperscript{247} So far Spain, Austria, Lichtenstein and Portugal have all chosen to extend intermediary immunity to cover any liability which may occur in relation to hyperlink (linking liability).\textsuperscript{248}

\textbf{5.2.4 The Notice and takedown procedure}

Unlike the DMCA, the ECD does not establish the notice and takedown procedure into statutory law. However, the ECD provides protection for ISPs who expeditiously take down claimed infringing material upon receiving notifications from copyright owners.\textsuperscript{249} This procedure stated in the ECD, falls short in many areas that can be found effective in the notice

\textsuperscript{246} See supra note 133, L. Edwards, p. 25.

\textsuperscript{247} Article 21(2) states that “In examining the need for an adaptation of this Directive, the report shall in particular analyze the need for proposal concerning the liability of providers of hyperlink and information location tool services,…….”

\textsuperscript{248} See supra note 133, L. Edwards, p. 25.

\textsuperscript{249} ECD. Article 14(1)(b).
and takedown procedure of the US regime. Due to the fact that the ECD does not adopt the notice and takedown procedure, difficulties have risen in many aspects concerning a constitution of knowledge standard, protection for ISPs where they takedown claimed infringing materials incorrectly on the basis of good faith, act of ISPs as a censorship body, freedom of expression and fair competition. As a result, compare to the DMCA, the ECD provides less legal certainty regarding rights and obligations for both ISPs and copyright owners. Nevertheless, the ECD purposes to leave room for Member States to implement the notice and takedown procedure in the form of code of conduct, meaning that the ECD does not affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information. In addition, similar to liability for information location tool provider, the European Commission is demanded to re-evaluate the need of adaptation the notice and takedown procedure.

5.2.5 Knowledge standard

Unlike the ECD, the DMCA codifies a knowledge standard for ISPs in a narrow fashion which made it difficult to manipulate. The DMCA establishes knowledge standard by setting requirements which have to be met in order to constitute actual knowledge. Furthermore, the DMCA also establishes constructive knowledge by following the red flag test. In this light, actual knowledge of ISPs can be perceived when they obtain notifications of claimed infringement from copyright owners. That is, the notification is a key factor which can constitute actual knowledge of ISPs. With regard to the notification, ISPs must set elements that have to be mentioned on the notification, as well as must designate the agent to whom such notification will be delivered. In return, copyright owners have to issue notifications which contain required information and submit it to a designated agent. If copyright owners fail to do so, it cannot be

---

250 These issues will be explained further in following paragraph.
252 ECD. Article 14(3).
253 See ibid. Article 21(2).
254 See supra note 82, C. Beams, p. 841.
255 DMCA. Section 512(c)(3)(B)(i)
assumed that ISPs have actual knowledge of infringing activity. In return, if ISPs do not provide required information nor designate the agent, they will not be eligible to take advantage of the safe harbor. On the other hand, because the ECD does not establish the notice and takedown procedure; it does not mention rules regarding the form or the content of notification and a clarification as to whom a notification should be submitted. According to constructive knowledge, the DMCA establishes awareness criterion which best described as red flag test, where as the ECD disregards to give a guideline concerning a criterion of awareness. This creates difficulties to judge whether ISPs have actual knowledge of claimed infringing activity or awareness of fact or circumstance of such activity.

5.2.6 Protection for ISPs who take down claimed infringing material with good faith

Under the notice and takedown procedure, ISPs are immunized from being held liable for any liability which may arise in relation to takedown procedure. The DMCA establishes a particular provision to protect ISPs where they take down claimed infringing material incorrectly on the basis of good faith. On the other hand, The ECD does not mention about this matter. According to article 14 of the ECD, ISPs are required taking down immediately upon receiving notifications of claimed infringing material from copyright owners, but there is no equivalent protection as the DMCA that ISPs will be protected from any liability where ISPs take down claimed infringing materials which they incorrectly believed to be illegal.

5.2.7 ISPs act as a censorship body

According to the notice and takedown procedure of the DMCA, ISPs has taken down allegedly infringing material, or disable access to it upon receiving notifications of claimed infringement without any investigation. As a result, it might force ISPs to act as a censorship body which they are not well equipped to do so. Moreover, in order for ISPs to take advantage

---

256 See ibid.
257 See ibid. Section 512(c)(2)(A)-(B).
259 DMCA. Section 512(g)(1).
of the safe harbor, ISPs must adopt and implement policy that provided for the termination of the internet access to alleged infringers. In this regard, ISPs have been convinced to terminate users’ the internet access on the basis of merely an allegation of copyright infringement, despite they have legal obligation to do so. The ECD, resembles the DMCA, according to article 14, ISPs must take down claimed infringing materials expeditiously upon receiving notifications from copyright owners. As explained in previous chapter, ISPs are not in an appropriate place to judge whether certain materials should be removed or should be made available publicly.

However, the DMCA, in this light, provides mechanism so-called put back regime. Therefore, to some extent, person whose material has been taken down has an opportunity to protest the action of ISPs and can initiate the process to put the material back online. As a result, it can imply that an authority of ISPs is not absolute. On the other hand, the ECD does not establish put back regime, and therefore under the ECD, it is up to ISPs to make decision whether certain materials should be removed or should be maintained online.

5.2.8 Freedom of expression and fair competition

The DMCA has taken the matter of freedom of expression and fair competition into account by including an elaborated notice and takedown procedure which gives an alleged infringer an opportunity to object and impose liability upon persons who knowingly misrepresent the infringement of copyright in order to reduce tons of notifications that have been given to ISPs for illegitimate reasons. The ECD, on the contrary, because of a non-existent of the notice and takedown procedure, lacks provisions concerning freedom of expression and fair competition. The ECD does not give alleged infringers an opportunity to protest the takedown, nor initiate the process to put the material back online. Besides, the ECD does not provide disincentive to persons who intentionally give false notifications to ISPs on inappropriate purposes either. However, the ECD is aware of these issues by stating in recital 46 that the removal or disabling of access has to be undertaken in the observance of the principle

---

260 See ibid. Section 512(g)(2)(A)-(C).
261 See ibid.
262 See ibid. Section 512(f).
of freedom of expression and of procedures established for the purpose at national level. It can imply that the matter of freedom of expression is taken into consideration, but the ECD leaves it to national law, instead of instituting it into the directive. Moreover, in practice, even though the ECD requires ISPs to concern about the matter of freedom of expression, it is naive to rely that ISPs will not remove claimed infringing material or disable access to it upon receiving notifications from copyright owners because they have to serve freedom of expression. Practically, ISPs tend to takedown as fast as possible in order to protect themselves from being held liable.\textsuperscript{263}

5.2.9 Duty to monitor and apply technologies

Both the DMCA and the ECD similarly state that ISPs will not be imposed a general obligation of monitoring their systems, and a generation obligation activity to seek facts or circumstances indicating illegal activity will not be imposed upon them either.\textsuperscript{264} According to the ECD, even though article 15 of the ECD constitutes strong statements, ISPs can, however, be forced to perform monitoring obligation in a specific case.\textsuperscript{265} Moreover, according to recital 48, the ECD does not affect possibility for Member States of requiring ISPs to apply duty of care in order to detect and prevent certain types of illegal activity, meaning that Member States might require ISPs to apply technologies to monitor their systems and indicate infringing materials such as filtering technologies.\textsuperscript{266} This recital appears to be in the contrary with article 15 which states that service providers, when transmitting, caching or hosting material are under no obligation to monitor such materials for signs indicating illegal activity. Consequently, even if the ECD provides a strong statement in article 15, there is a problem of reconciling other provisions which seem to be in contradiction with general principle.

\textsuperscript{263} See supra note 164, R. Julia-Barcelo & K Koelman, pp. 232-233.
\textsuperscript{264} DMCA. Section 512(m) and ECD. Article 15
\textsuperscript{265} See ibid. Recital 47.
Likewise, the DMCA clarifies that ISPs are not obliged to monitor their sites for infringing materials. However, the exclusion of an obligation to monitor is not absolute. In this regard, in order for ISPs to take advantage of the safe harbor, they must comply with requirements in which they must accommodate and not interfere with (future) standard technical measures that are utilized by copyright owners to identify or protect copyright works. As a result, the availability of such technical measures may result in a duty of monitoring content that transmitted, cached or hosted materials or the content to which one provides hyperlink. Hence, the availability of technologies that facilitate monitoring may broaden the scope of ISP’s duty, meaning that the availability of technologies might impose upon ISPs an obligation of monitoring their systems. Consequently, even though, both regulations do not impose a general obligation of monitoring upon ISPs, there are provisions that can imply that ISPs, in special case, have to bear responsibility of monitoring their systems.

5.2.10 Existing law and national law remain intact.

The DMCA does not make ISPs liable automatically, if certain activities, performed by ISPs, do not fall within provisions of the safe harbor. In other words, it does not mention that ISPs have to follow the DMCA otherwise they will be held liable; instead, ISPs may choose to claim the DMCA or choose to follow the existing law. The ECD, on the other hand, was regulated separately; however, it mostly does not affect authority of national laws. That is the ECD leaves room for Member States to have the possibility to order any kinds of injunction, establish methods to prevent infringement or terminate infringers, or institute procedures concerning preventive measures in accordance with their national laws. This means that even though the ECD requires Member States to impose the directive into their national legislations, national laws remain untouched and cannot be influenced completely by the ECD. As a result,

---

267 DMCA. Section 512(m).
268 See ibid. Section 512(i)(1)(B).
269 See ibid. Section 512 (m)(1) states that nothing in this section shall be construed to condition the applicability of subsection(a) through (d) on (1) a service provider monitoring its service or affirmative seeking facts or indicating infringing activity, except to the extent consistent with a standard technical measure...
270 See supra note 3, K. Koelman p. 34.
either the DMCA or the ECD cannot do their best to provide legal certainty for ISPs as long as they are restricted by existing laws or national laws.

5.4 The DMCA loopholes

5.4.1 The DMCA provisions are based on specific, outdated technology and do not provide sufficiently flexible basis for regulating fast-evolving technologies

In the field of copyright liability, a new class of online intermediaries has emerged which were largely not in the minds of legislators at the time of drafting of leading immunity instruments in the late 1990s. Peer-to-Peer file sharing technology (P2P) was in widespread after the DMCA provisions had been created. As a result, they do not account for file sharing activity. Apparently, The DMCA establishes the extent of activities of ISPs which can take advantage from safe harbor only when infringements involve four functions: transitory network transmission, caching, storage of material on behalf of users and information location tools. Each of these functions, however, is narrowly defined by the statute. Therefore, P2P software is not protected by the safe harbor. As abovementioned case, the Napster could not claim that it performed passive conduit activity unless claimed infringing information passed through its own private network. According to Napster, the software operated by connecting internet users with its central server. ISP in this case only provided internet connectivity which would actually fall within section 512(a) of the DMCA, but the court ruled that Napster was not a service provider according to section 512(k)(1)(A) of the DMCA, and therefore Napster could not take advantage of the safe harbor. Moreover, supposing the DMCA could be applied to P2P situation, according to section 512(c), it requires ISPs to remove claimed infringing material or disable such material which resides in their networks, upon obtaining notification. This is quite problematic when applying to P2P architecture because according to the operations of P2P, material does not reside in ISPs’ networks; instead on users’ computer which ISPs have no


control of. Consequently, a lack of provisions to protect ISPs in this situation is likely to impede an investment in new technology and innovation.\(^{274}\)

5.4.2 The Safe harbor creates the problem of freedom of expression

Numerous commentators have expressed concerned that the DMCA’s safe harbor provisions potentially infringe freedom of expression rights of internet users.\(^{275}\) Even though the DMCA provides persons whose materials has been taken down an opportunity to protest and initiate the process that allows them to put their materials back online,\(^{276}\) the process that designed to protect them found inadequate. In practice, when claimed infringing material is taken down, it usually happens before not only a judge reviews the complaint, but also before an alleged infringer is informed about such action. In this light, even if the DMCA provides mechanisms to protest against the complaint by submitting a counter-notification, when the material has been taken down it must stay down for 10-14 days.\(^{277}\) Ten days or two weeks may greatly diminish the value of the time-sensitive information.\(^{278}\)

5.4.3 The safe harbor protection is dangerous for online business

The safe harbor might give a negative effect to online business. With regard to the notice and takedown procedure, ISPs seem to take down allegedly infringing material, disable access to such material or shut down an allegedly infringing website with little or no investigation since ISPs want to be excluded from being imposed liability. In this light, it appears that ISPs are overzealous in taking down certain materials in attempt to avoid liability.\(^{279}\)

\(^{274}\) See supra note 133, L. Edwards, p.7.


\(^{276}\) DMCA. Section 512 (g)(2)(A)-(C).

\(^{277}\) See ibid. Section 512 (g)(2)(C).


abovementioned, once allegedly infringing material has been taken down, it must stay down for 10-14 days. As a result, this process might result in a chilling effect on commercial enterprise doing business on the internet since they would face serious damage from being taken off line for two weeks.  

5.4.4 The problem of termination allegedly repeat infringers’ the internet access

ISPs will be eligible to take advantage of the safe harbor when they have adopted and reasonably implemented a policy that provided for the termination of the internet access for persons who are repeat infringers.  This article has convinced ISPs to terminate their subscribers’ the internet access on the basis of merely allegation of copyright infringement, even though there is no legal obligation to do so. Moreover, the DMCA does not define repeat infringers and no case has been brought on this point yet. As a result, it could threaten internet users’ ability to access the internet.  

5.5 The ECD loopholes

When compared to the DMCA, the ECD comes up somewhat short in some areas. The main loopholes of the ECD is that First, it does not establish the notice and take down procedure, and therefore it creates problems of knowledge standard, protection of ISPs where they takedown claimed infringing material on the basis of good faith, freedom of expression and fair competition. Second, the ECD does not establish immunity for information location tool providers. Finally, the ECD itself has problem of conflict provisions concerning a general obligation to monitor.

5.5.1 No the notice and take down procedure

Apparently the ECD does not establish the notice and takedown procedure, and therefore it results in little guidance or protection for ISPs in the removal or restoration of

---

280 See supra note 279, R. Polk Wagner.
281 DMCA. Section 512(i)(1)(A)
282 See supra note 272, Electronic Frontier Foundation report.
283 See ibid.
In this regard, lacking of the notice and take down procedure means less legal certainty is provided. As for ISPs, legal certainty is very important because it is crucial for ISPs to know what procedures exempt them from liability so that they can avoid being in the doubtful position.

As noted earlier, the ECD requires ISPs to takedown claimed infringing materials upon gaining actual knowledge or constructive knowledge, but the ECD does not provide criterion of what either actual knowledge or constructive knowledge is. Therefore, it has resulted in difficulties in order to judge whether ISPs have actual knowledge or awareness of facts or circumstances of infringing activity.

Another problem is that the ECD seems to disregard the matter of freedom of expression since the ECD does not provide persons whose material have been taken down an opportunity to protest or initiate the process to put materials back online. Nevertheless, even if the ECD does not codify this matter into any provision of the ECD, it provides Member States the possibility to establish any requirements concerning the principle of freedom of expression which must be fulfilled prior to the takedown. However, as explained above, ISPs are likely to expeditiously takedown upon receiving notifications. It is relatively impossible that they will take the matter of freedom of expression as the first priority. Moreover, the ECD does not allocate liability upon copyright owners who intentionally give fault notifications to ISPs in order to exploit quick reaction of ISPs upon receiving such notifications. This might be an impetus for malicious-minded copyright owners who want to eliminate competition in business by giving incorrect notification to ISPs.

However, even though the ECD does not codify the notice and takedown in the regulation, it leaves room for Member States with the discretion to institute procedure governing the removal or disabling of access to information. Furthermore, the ECD should adopt the notice

---

284 See supra note 101, V. McEvedy. p.3.
285 ECD. Recital 45
286 ECD. Article 14(3)
and takedown from the US regime which can do so on the basis of article 21(2) that requires the European Commission to consider the need of the notice and takedown procedure and re-evaluate whether it should be adopted. However, one legal commentator suggests that it would not be appropriate to constitute the notice and takedown procedure into the ECD since the ECD does not establish provisions concerning a put back procedure, nor provision regarding allocation liability upon copyright owners who intentionally give false notifications of claimed infringing material. Lacking those provisions, it is not proper to codify the notice and takedown procedure into the directive. The legal commentator suggests that the European Commission should consider the creation of special body which all complaints will be directed to. The body has duty to verify notifications, and if after considering and coming to the decision that notification is justified; the body will require ISPs to take infringing material down. To let the special body operate the verification is also providing protection for freedom of expression since it does not depend on ISPs to judge whether certain material should be kept or maintained online. In this sense, an operation of the special body will lessen authority of ISPs.

5.5.2 No protection for ISPs who provide information location tool services

The ECD provides immunity for the performances of ISPs in the storage of information in the case of transitory storage, caching, the storage of information on behalf of third parties (hosting), but surprisingly it does not mention about protection for ISPs who provide information location tool services. This pitfall of the ECD might affect the development of e-commerce since ISPs will hesitate to provide information location tool services where they are not provided immunity. As abovementioned, however, the European Commission has to take the issue of liability of providers of hyperlinks and location tool services into account, and re-evaluate the need of this protection.

287 See supra note 164, R. Julia-Barcelo & K Koelman, p. 237
288 See supra note 19, P. Basicrocchi, p. 130.
289 ECD. Article 21(2)


5.5.3 Problem of general obligation to monitor

Despite the ECD strongly states that Member States are prohibited to neither impose upon ISPs a general obligation of monitoring their systems, nor require ISPs to seek facts or circumstances indicating illegal activity, there is a recital of the ECD that appears to be in contradiction of the general principle. According to recital 48, it states that even though ISPs will not be imposed upon general obligation of monitoring their systems, it does not affect the possibility of Member States of requiring ISPs to apply duty of care to detect illegal material. A broad interpretation of this recital may hinder a clear and uniform application of article 15. As a result of this inconsistency, some legal commentator suggests that the recital 48 should not be taken into account. Moreover, articles 12-14, state that each article does not affect the possibility for a court or administrative authority of requiring ISPs to terminate or prevent an infringement. Therefore those provisions could also undermine the application of article 15. Moreover, the issuance of injunction that requires ISPs to prevent infringement could result in an obligation of monitoring since ISPs, upon receiving injunction from the courts, might utilize technologies to observe their site and seek for illegal activity. Moreover, from national case laws, courts have a tendency to be inspired by recital 48 which enables them to issue injunctions that require ISPs to bear general responsibility of monitoring their system.

5.5.4 Authority of National laws

According to the ECD, it leaves room for Member States to impose their own national laws. Articles 12-14 does not affect possibility of Member States to initiate their procedures to deal with copyright infringement prevention, or to establish the process of removal or disabling alleged infringing material. Moreover, according to recital 45, 46, 47, 48, as abovementioned, the ECD is likely to rely to Member States to establish measures to deal with detecting copyright infringement, protecting freedom of expression, as well as the notice and take down

---

290 See supra note 164, R. Julia-Barcelo & K Koelman, pp. 232.
291 See supra note 163, P. Eecke & B. Ooms, p. 5(citing C. De Preter, Wie heef nog boodschap aan de boodschap? De aansprakelijkheid van tussenpersonen onder de wet elektronische handel,(2003), p. 266.)
292 ECD. Article 12(3), 13(2), 14(3).
293 See supra note 163, P. Eecke & B. Ooms, p. 6.
294 See e.g. SABAM and IFPI v. Seniorennet (Belgium), Rolex v. Ebay (Germany).
295 ECD. Articles 12(3), 13(2), 14(3).
procedures instead of instituting those measures into the ECD itself. In other words, those measures are encouraged to be settled in the form of a code of conduct. Hence, it can conclude that the ECD does not provide a complete protective mantle for ISP as long as national laws give effect more than the ECD does.

5.6 Conclusion
In summary, according to the comparison, the DMCA and the ECD provide a generally similar protection so-called the safe harbor, as well as establish the conditions that ISPs must comply with in order to benefit from the safe harbor protection. Nevertheless, the ECD is found to be lacking in some areas when compared to the DMCA. The main thing is that the ECD does not provide immunity for information location tool providers, nor establishes the notice and takedown procedure. As a result of lacking such provisions, it results in less protection and unstable legal certainty for ISPs. The DMCA, when compare to the ECD, is more preventive as it covers more certain functions performed by ISPs that can be exempted from being held liable. Moreover, the DMCA establishes the notice and take down procedure which is very crucial for ISPs to know their rights and obligations. Therefore, ISPs under the DMCA is more protective than the ECD.
Chapter 6
Concluding remark

6.1 Introduction
This chapter will conclude advantages and drawbacks of both the DMCA and the ECD, as well as suggest proposed recommendations that can enhance both legislations. The last paragraph will answer the research question.

6.2 The DMCA

Advantages
ISPs can be seen as potential defendants under copyright legal doctrines of the Copyright Act which imposes liability upon ISPs unjustifiably. ISPs have been left unprotected and faced with unclear situation that to what extent they should be responsible for copyright infringement committed by others. The DMCA has generally proved reasonably effective and addressed controversial issues. The DMCA provides legal certainty for ISPs and make them secure to stay in business.\(^\text{296}\) ISPs under the DMCA are protected by the safe harbor regime. The DMCA establishes provisions concerning functions of ISPs that fall within the safe harbor, and therefore ISPs can be shielded from being held liable. In this way, ISPs can be certain that they cannot be potential defendants where they merely play a role as passive conduit of a transmission of information. Hence, direct liability will be unjustified to impose upon ISPs under the DMCA. Moreover, the DMCA establishes knowledge standard in narrow fashion which is clear and hard to be stipulated. Actual knowledge can be perceived when ISPs obtain notifications of claimed infringement from copyright owners while constructive knowledge can be judged by the red flag test. In this light, the constructive knowledge is not the same standard as existed in required factor of contributory liability but narrower. Furthermore, the notice and takedown procedure, in my view, is a very well drafted, even though there are some problems which occurred in relation to the implementation of the procedure. The advantages of the

notice and takedown procedure outweigh the drawbacks. The benefits of the procedure are
that; first, the procedure encourages ISPs and copyright owners to combat copyright
infringement by providing incentives for both parties. In this way, copyright owners give
notifications of claimed infringement to ISPs so that ISPs can take down such materials;
copyright owners benefit from action of ISPs. In return, when ISPs expeditiously takedown
claimed infringing material, they can be protected under the DMCA.

Second, ISPs are less concerned about any liability which might occur in relation to takedown
allegedly infringing material since the DMCA provides immunity for ISPs who take down such
material on the basis of good faith.

Third, the notice and takedown procedure provides persons whose materials has been taken
down an opportunity to protest and initiate the process to put materials back online, and this
provision can assume that the DMCA takes the issue of freedom of expression in to account.
Moreover, the DMCA allocate liability upon malicious-minded copyright owners who
intentionally give false notifications to ISPs. Therefore, it can eliminate unfair competition and
can reduce a number of inappropriate notifications.

Finally, the DMCA does not require ISPs generally obligation of monitoring, nor apply
technology to police their systems. It is sensible for ISPs because it is burdensome for ISPs to
bear such responsibility.

**Drawbacks**

However, there is contrary view of the DMCA concerning the safe harbor and the notice and
take down procedure.\textsuperscript{297} The argument suggests that it was not necessary to adopting the

\textsuperscript{297} See e.g. A. Yen, (2002), ‘Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise
‘Safe Harbors Against the Liability Hurricane: the Communications Decency Act and the Digital Millennium
Forward, Two Steps Back: An Historical Analysis of Copyright Liability’, *Cardozo Arts & Entertainment Law
DMCA because, First the DMCA prevented future judicial clarification because when the DMCA has been adopted, a wide spread use of the safe harbor procedure will bar an opportunity that lets the court decide cases clarifying liability of ISPs.

Second, the safe harbors protection that gives incentive to ISPs to be exempted from being held liable creates excessive authority for ISPs regarding takedown procedure. In this regard, the notice and take down leads to the following problems: (1) as noted above, ISPs respond immediately to take down claimed infringing material merely on the basis of allegation of copyright infringement, meaning that certain material has been taken down before it was verified. Therefore, it has resulted in problems of freedom of expression and could impede the development of online businesses. However, even thought, the DMCA takes these matter into account by provide an opportunity for one whose material has been taken down to protest and initiate the process to put the material back online, the procedure found insufficient to safeguard freedom of expression since the material might have been down for 10 or 14 days. Hence, it could create damages in cases of sensitive information, as well as a huge loss in online business; (2) in case of repeat infringer, the DMCA seems to encourage ISPs to terminate users’ the internet access merely on the basis of allegation of copyright infringement. In addition, the DMCA does not define repeat infringer. As a result of this, it could threaten users’ ability to access to the internet.

Third, the emergence of new kinds of intermediary does not fit in the safe harbors protection, even if their functions fall within the safe harbor. In this respect, P2P system is the best example; in the case of Napster, ISP merely provided connectivity to users which would actually fall within the first safe harbor, but court refused to grant the safe harbor protection as an operation of Napster was not be considered as an service provider under the DMCA. According to the definition of ISP, courts tended to define it narrowly and did not want to extend a scope of definition. Hence, this old-fashion regulation might give negative effects to a development of new technologies and utilization of new innovation.
Recommendation
The DMCA should be reconsidered and amended in order to keep it up to date. First, the four safe harbors should be considered extending function of ISPs that should be protected, as well as the scope of definition. Second, the authority of ISPs to judge whether which material should be removed or maintained should be lessened by establishing special body. As one legal commentator suggests that the ECD should create special body, I think the DMCA should also consider this matter. Even though the DMCA has a higher protection of supporting freedom of expression than the ECD, as noted above the procedure is not good enough. In my view, ISPs should not be given an obligation to judge whether certain materials should be taken down, but the notification of claimed infringement should be delivered to a special body, then the body will verify and if the notification is justified, ISPs will be informed to take certain materials down. In this respect, it will be fair for persons whose materials have been taken down that their materials will be taken down merely when such materials have been verified. Moreover, the DMCA should explicitly define some wording which is likely to be problematic in practice, such as good faith, repeat infringer or awareness.

6.3 The ECD
Advantages
The ECD was enacted on the purpose of enhancing the growth of e-commerce in the internal market. The main goal of the ECD is to provide legal certainty for entrepreneurs doing businesses online, as well as build up consumer confidence when they have to deal with online business. As a result, the ECD have to harmonize laws among Member States in order to eliminate disparities which can impede the development of cross-border services. The matter of ISP liability is one of the original issues which is established in section 4 of the ECD on the purpose of providing certainty for ISPs when they are involved in third-party copyright infringement. The ECD establishes extent of liability that can be imposed upon ISPs, that is ISPs will be held liable if certain functions performed by ISPs do not fall within the limitations of liability provided in the ECD. The ECD provides the safe harbor for ISPs in the same manner as

298 See supra note 164, R. Julia-Barcelo & K Koelman, p. 237.
the DMCA does, as well as set forth the conditions that ISPs have to be met so that they can benefit from the safe harbor protection. Moreover, the ECD excludes ISPs from being imposed a general obligation of policing their networks. Furthermore, the ECD establishes the procedure which is somewhat similar to the notice and take down procedure of the US regime. With regard to article 14 of the ECD, it requires ISPs who gain actual knowledge or awareness of facts or circumstances of infringing activity expeditiously take down claimed infringing material.

**Drawbacks**

However, the ECD comes up short in some issues when compared to the DMCA. First the ECD does not provide protection for ISPs who provide information location tool services.

Second, As noted above, the ECD did not adopt the notice and take down procedure, therefore it creates the following problems: (1) the ECD lacks of what constitutes knowledge of ISPs, what elements should be mentioned in notifications of claimed infringement, and to whom notifications should be delivered; (2) the ECD does not serve freedom of expression as it does not offer persons whose materials have been taken down an opportunity to protest, nor initiate the process to put materials back online, and therefore it results in a censorship body that ISPs became; (3) the ECD does not provide immunity for ISPs who take down claimed infringing materials upon receiving notifications from copyright owners on the basis of good faith; (4) the ECD does not allocate liability upon malicious-minded copyright owners who intentionally give incorrect notifications in order to eliminate their competitive parties by exploiting fast action of ISPs.

Third, even though the ECD prohibits Member States to impose a general obligation of monitoring, the ECD contains provisions that appear to contradict with article 15, and therefore they could undermine an effectiveness of the main principle.299

---

Nevertheless, although the ECD does not institute crucial matter into the directive itself, the ECD does not affect possibility for Member States of establishing any measure/procedure dealing with those issues in accordance with national laws. First, with regard to the notice and take down procedure, the ECD does not affect possibility for Member States of establishing procedure governing the removal or disabling of access to information. Second, concerning freedom of expression, the ECD does not affect Member States’ possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information. However, to leave room for national laws means the ECD is not implemented absolutely. Member States anytime can always impose their own ways to deal with issues. Hence, it can conclude that the ECD does not provide a complete protective immunity for ISPs.

**Recommendation**

As aforementioned, the ECD does not affect possibility for Member State of establishing preventive measures or procedures in accordance with national law. Therefore, the ECD should instead of amending the directive itself, encourage Member States to draw code of conducts concerning lacking issues which closely conform to the ECD. Moreover, article 21(2) instructs the European commission to re-examine the need of adopting concerned issues such as the notice and take down procedure and protection for ISPs who provide information location tool services. Furthermore, in order to achieve an effective implementation of the ECD, the European Commission should provide a guideline regarding how to interpret provisions of the regulation, how to apply provisions which seems to contrast to each other or how to reconcile them harmoniously. Moreover, as noted above, according to the notice and take down procedure, one legal commentator suggest that the European commission should take into account the creation of special body instead of adopting the notice and take down procedure since the ECD does not establish protection for ISPs who wrongfully believe that they takedown an illegal material, nor impose liability to parties who intentionally give false notifications to ISPs. Therefore, it might not appropriate to adopt the notice and take down, but the European Commission would rather institute the special body which operates by verifying claimed

---

300 ECD. Article 14(3).
301 See ibid. Recital 46.
infringing material notification, then after it is justified, ISPs will be informed to takedown. Therefore it could get rid of an absolute authority of ISPs of judging which material should be kept or should be removed.

6.4 To what extent should ISPs be held liable for third-party copyright infringement?

The extent of liability which will be imposed upon ISPs is limited by certain functions performed by ISPs and the conditions that ISPs must obey in order to take advantage of limitations of liability. The US and the EU regimes, in my view, are averagely successful of providing legal certainty for ISPs. ISPs are provided a clear framework of what constitutes liability, and what they must do in order to be immunized. However, both regulations need improving in order to respond to rapidly growth of technologies which always brings new issues. Moreover, clarifying provisions has to be taken into account too.
Bibliography

Books


Articles


83, No. 4.

Journal of Information, Law and Technology (JILT), issue 3.

WIPO to Establish International Copyright Procedural Guidelines for Internet Service

Law & the Arts, Vol. 24, No.1.


Communication Law, Vol. 7, No. 3.

Communications Decency Act and the Digital Millennium Copyright Act’, Cardozo Arts &

28. J. Harper, (2005), ‘Telecommunication & Technology- Against ISP liability- Do ISPs have a
duty to protect the world?, ALI journal on government and society, Vol. 28, No. 1.


under Section 512 of The Digital Millennium Copyright Act’, 22 Santa Clara Computer &

31. J. Hoboken, (2009), ‘Legal space for innovative ordering: On the need to update
selection intermediary liability in the EU’, International Journal of Communication Law &


WIPO workshop


Internet


David Kravets, 10 Years Later, Misunderstood DMCA is the Law That Saved the Web, available at http://www.wired.com/threatlevel/2008/10/ten-years-later/


FAQ about DMCA safe harbor, available at http://www.chillingeffects.org/dmca512/faq.cgi


