Internet Service Providers’ liability concerning copyright infringements on the Internet

Sandra Djordjevic

SCHOOL OF ECONOMICS, BUSINESS ADMINISTRATION & LEGAL STUDIES
A thesis submitted for the degree of
Master of Arts (MA) in Art, Law and Economy

February 2018
Thessaloniki – Greece
Student Name: Sandra Djordjevic
SID: 2202160003
Supervisor: Prof. Irini A. Stamatoudi

I hereby declare that the work submitted is mine and that where I have made use of another’s work, I have attributed the source(s) according to the Regulations set in the Student’s Handbook.

February 2018
Thessaloniki - Greece
This dissertation was written as part of the MA in Art, Law and Economy at the International Hellenic University.

The Internet has become a part of our everyday life. It has enhanced and enriched our lives making it possible for us to access information from anywhere in the world in the blink of an eye. However, it has also been used for illegal activities such as sharing copyright protected works without authorization, thus leading to the widespread of cyberpiracy.

In an effort to protect their rights, copyright holders turned to ISPs as providers of information services for help to identify the infringers by revealing their users’ personal data in order to initiate proceedings against them. Occasionally, right holders held ISPs liable for copyright infringements as enablers of service which was used to perform an illegal act.

This further led to the collision of the fundamental rights to privacy, to conduct business, to protect property and the freedom of expression. As it threatened to endanger EU Single Market, the European Union attempted to establish a desired balance among fundamental rights through legal regulations and CJEU case law.

The focus of this paper is on the legal status and liability of ISPs in the process of unauthorized distribution of copyright protected works in digital environment by using services they provide.

Through examination of relevant regulations and case law, this paper proposes that the solution to the problem of digital piracy, without disturbing the balance of fundamental rights and neutral status of ISPs’ can be found by combining legal provisions, the advantages of innovative technologies and educational measures.

**Keywords:** Internet service provider, secondary liability, copyright infringement, digital piracy, E-Commerce Directive, CJEU case law

Sandra Djordjevic
15 February 2018
First, I would like to thank my mentor Professor Irini A. Stamatoudi for her time, knowledge and experience invested in this dissertation. I would like to pay special thanks to the International Hellenic University and their staff for understanding and encouragement they provided. In addition, I would like to express gratitude to the Greek Ministry of Education, Research and Religious Affairs and Greek Consulate in Belgrade for making it possible to experience life and study in Greece. I would like to thank the foundation “Dositej Obradovic” for supporting my vision and providing necessary assistance. I would also like to thank the Dean of the University of Belgrade Faculty of Law, Professor Sima Avramovic and the entire academic staff of the faculty. And last but not least, I would like to thank my mother and father, family Dragicevic, Appellate Court judge Smiljka Dingarac and my fellow colleagues for their ongoing love, support and encouragement.

Sandra Djordjevic

15 February 2018
# Table of Contents

**Abstract** ............................................................................................................................................. 1

**Acknowledgments** ................................................................................................................................. 2

**Table of Contents** .................................................................................................................................. 3

**Abbreviations** ....................................................................................................................................... 6

**Introduction** .......................................................................................................................................... 7

## 1 Opening Remarks

1.1 Digital piracy as a background story of ISPs’ liability for copyright infringements........................................ 9

1.2 Who to blame for unauthorised online sharing of copyright protected works – users or ISPs? ......................................................... 9

1.3 How did ISPs get in the midst of the battle between the right to property and the right to privacy?.............................. 10

1.4 Why are ISPs not disclosing users’ personal data? .................................................................................. 11

## 2 EU Legal Framework on the Liability of ISPs

2.1 Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-Commerce Directive) ................................................................. 12

2.1.1 The aim of the Directive .................................................................................................................. 12

Exemptions from ISPs’ liability

2.1.2 Mere conduit (Article 12 of the E-Commerce Directive) ................................................................ 13

2.1.3 Caching (Article 13 of the E-Commerce Directive) ....................................................................... 13

2.1.4 Hosting (Article 14 of the E-commerce Directive) ......................................................................... 15

2.1.5 Gaps and positive aspects .............................................................................................................. 16

3 EU LEGAL FRAMEWORK REGULATING THE HARMONIZATION OF COPYRIGHT AND RELATED RIGHTS AND THE ENFORCEMENT OF INTELLECTUAL PROPERTY RIGHTS

3.1 Harmonising copyright and related rights in the EU information society...........21
3.2 Enforcing IPRs in the digital environment...........................................................22

4 EU LEGAL FRAMEWORK REGULATING THE PROTECTION OF PRIVACY AND PROCESSING OF PERSONAL DATA

4.1 Protection of individuals in the processing of personal data...............................24
4.2 Processing of personal data and the protection of privacy in the electronic communications sector..........................................................26
4.3 General Data Protection.......................................................................................27

5. CJEU CASE LAW

5.1 Searching for a balance between fundamental rights through the case

   *Productore de musica de Espana (Promusicae) v Telefonica de Espana (C 275/06)*..............................................................30

   5.1.1 Background and the issue...........................................................................30
   5.1.2 Court ruling and effects on the liability of ISPs........................................30

5.2 Providing access to the Internet is enough to constitute ISP’s secondary liability in the case *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH (C-557/07)*..............................................32

   5.2.1 Background and the issue...........................................................................32
   5.2.2 Court ruling and effects on the liability of ISPs........................................33

5.3 Confirming prohibition of obligation of general monitoring by ISPs in the case *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (C-70/10)*............................................................34

   5.3.1 Background and the issue...........................................................................34
   5.3.2 Court ruling and effects on the liability of ISPs........................................35

5.4 Additional prohibition of general monitoring obligation by hosting providers in the case *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV (C 360/10)*.................................................................................36

   5.4.1 Background and the issue...........................................................................36
   5.4.2 Court ruling and effects on the liability of ISPs........................................36
5.5 CJEU allows national court to adjudicate ‘open-textured’ remedies towards ISPs in the case *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH (Case C-314/12)*……………………………………………………37

5.5.1 Background and the issue………………………………………………………………………………………………37

5.5.2 Court ruling and effects on the liability of ISPs…………………………………………………………………………………………………………………………38

5.6 Extending the reach of awarded injunctions to future infringements through the case *L’Oréal SA and others v eBay International AG and Others (324/09)*…………40

5.6.1 Background and the issue……………………………………………………………………………………………………………………40

5.6.2 Court ruling and effects on the liability of ISPs……………………………………………………………………………………………………………………40

6 MECHANISMS AGAINST ONLINE COPYRIGHT INFRINGEMENT

6.1 Law-based mechanism – the French HADOPI Law……………………………………………………42

6.2 Soft law mechanism – Dutch ‘Notice and Take Down’ Code of Conduct……………………45

6.3 Mechanism established by a private entity – Content ID……………………………………48

7 CONCLUSION………………………………………………………………………………………………………………………………………………..52

8 BIBLIOGRAPHY…………………………………………………………………………………………………………………………………………54
ABBREVIATIONS

CJEU – Court of Justice of the European Union

CRT - Content Recognition Technology

HADOPI - Haute Autorité pour la Diffusion des Oeuvres et la Protection des Droits sur Internet

IP address – Internet Protocol address

IPR – Intellectual property right

ISP – Internet service provider

LSSI - Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico

UMG – Universal Music Group

WMG – Warner Music Group
INTRODUCTION

The development of cyberspace and digital technologies has impacted the creation and distribution of copyright-protected works. It made it possible for the copyright protected works to reach wider public, however, it also lessened the control of the right holders have over their publication and communication. In recent years technology has enabled flourishing of unauthorised cross-border distribution of protected works. The appearance of large-scale piracy has impacted not only individuals but also the EU Single Market. Due to such extensive impact, the EU was determined to take necessary steps to restore the proper functioning of Single Market, through harmonization of copyright and its enforcement.

Additionally, the EU has a great interest in resolving cyber piracy as a part of the Digital Single Market Strategy. Through this Strategy, the EU is hoping to create a fair competition business environment by making use of digital tools, which is to say that cyber infringements of copyright must be resolved.¹

However, the solution turned out to be more complex than expected due to specific interests of different stakeholders. The ultimate solution had to satisfy the right holders and their right to control their work, without disrupting the functioning of the Internet, which meant allowing ISPs to freely conduct their business and for users to remain anonymous. In order to ensure uninterrupted functioning of the Internet, the EU established a legal immunity for ISPs in cases where their role was purely technical and automatic without intentional interference with the content.

On the other hand, the right holders wanted to identify infringers in order to bring proceedings against them, however, they realised that such quest was arduous in an anonymous, cyber environment. Therefore, they turned to ISPs. In an online environment, ISPs enable communication by connecting users or hosting content provided by third parties. Right holders requested the ISPs, to help them identify users who were illegally communicating their work and/or to be held secondary liable for copyright infringement, as they were the enablers of the illegal act of communication.

The ISPs were reluctant to reveal the identity of their users, due to provisions protecting the privacy of personal data and fear of losing clients. This puzzling situation has led to numerous cases before the CJEU in search for a balance of the fundamental rights to property, privacy and freedom to conduct business.

The aim of this paper is to provide an insight into ISPs’ liability for the infringing content provided online by a third party using ISP’s services under EU legislation. In order to fully understand the position of ISPs, this paper will also analyse legal framework regulating rights and interests of other stakeholders such as copyright right holders and the users of ISP’s services.

The first part presents the EU legal framework governing the status of stakeholders involved in copyright infringement. Each stakeholder strives to protect their own interest, which creates a tension that the EU tried to balance and harmonise through multiple directives.

The second part is devoted to the CJEU case law, providing an insight into the manner in which these directives were interpreted in specific cases. Through case law the Member States were given additional specified guidelines on how to interpret and transpose directives into national legislation.

The third part provides examples of mechanisms chosen by Member States and private entities in order to incorporate provisions and court judgments regulating ISPs’ liability while respecting challenges that each of them encountered within their national legislative system in the process of balancing interests and requests of stakeholders.
1. OPENING REMARKS

1.1 Digital piracy as a background story of ISPs’ liability for copyright infringements

The issue of ISPs liability for copyright infringement is interconnected with digital piracy. Digital piracy can be defined as an unauthorised performance of any act which is considered to be an exclusive right of the right holder by using the Internet whether for lucrative purposes or not.

The Digital Age has allowed for the production of copies of copyright-protected work without any disturbance to the quality of the sound and/or image, with marginal costs and no need for physical carriers of the copies. The internet has made the access to and the transfer of said work possible at the speed of light from one side of the globe to another. This presents a fertile ground for digital piracy.

Even though the right holders are granted limited legal monopoly on reproduction and distribution of the work, these rights have become difficult to enforce in the digital environment. Once the work appears online, it is generally impossible to remove every copy or to block its further distribution.

Consequently, this disturbed the right holders’ monopoly, by allocating resources from right holders to infringers and thus affecting the market. There has been a need for legal reaction at the EU level not only to protect the rights of the right holders but also to restore order in the internal market.

1.2 Who to blame for unauthorized online sharing of copyright protected works - users or ISPs?

An ISP is a legal entity providing services, to its clients against a contract based fee. It can provide a connection to the network by connecting clients to the server (access provider), facilitate data transmission by providing technical services (network provider) or
rent space on its own server for users to upload content (host provider).\(^2\) Due to the development of the Internet, these services are not easily distinguished today.

The distinction has to be made between the secondary and primary liability of ISPs. Primary liability means that an ISP, a natural or legal entity, has performed an act of copyright infringement. Secondary liability means, that there is no direct line between an ISP and the act of infringement; however, the ISP has in some form enabled or facilitated this infringement. In P2P file sharing, an ISP as an access provider has provided a connection which was used to transfer infringing files. As a host provider it provided space in which the infringing material was made available to the public.

Furthermore, if infringing content is shared by a user, regardless of whether it is a P2P file sharing or if it is made available on a specific site, the user, as the content provider, is directly liable. However, a problem arises as the identification of the user is not so simple. In a digital environment, users are represented by an IP addresses which are assigned to them every time they log on. IP address is a combination of numbers meaningless to an ordinary person. However, a service provider can decode the IP address and translate it into personal data such as name, address, age etc. The data assigned to the IP address is unmistakably personal data within the meaning of Article 2(a) of the Directive 95/46 due to this connection to a specific person.\(^3\) This means that other users remain anonymous for the rest of us, while the ISP can perform the operation of identification of their users and determine their true identity.

**1.3 How did ISPs get in the midst of the battle between the right to property and the right to privacy?**

This happened for several reasons. Firstly, ISP provides ‘tools’ which enable unauthorized distribution of copyright-protected work and is in the best technical position

---


to block distribution. Secondly, ISP can identify the infringer and make it possible for right holders to legally prosecute by handing over personal information. Thirdly, right holders realized how difficult it is to find and prosecute the end users due to the problems regarding the disclosure of private data, and that it is far easier to go after the ISPs as ‘enablers’ since these infringements would have been impossible without the ISPs’ services. A legal ground for this claim was found on the basis of ‘strict liability’ theory, stating that negligence or omission of certain acts can be considered as an act of infringement.

1.4 Why are ISPs not disclosing users’ personal data?

Strictly speaking, an ISP can disclose personal data regarding the infringer. They are in the possession of a technology to do so easily.

However, no right exists without limitations. The right to property and the right to effective protection of property (right to effective remedies) are limited in a sense by the right to privacy and confidentiality of communication. Personal data is considered as sensitive data and should not be disclosed easily as it can negatively impact the data subject if fallen in the wrong hands. Legislation does allow for the disclosure of personal data, however in a limited number of occasions and under a strict procedure performed by an appropriate authority.

Regulations and case law reviewed in this paper are an attempt to find the adequate balance between these rights and resolve the problem of who should be considered liable for online infringements. However, none of them have given a definite solution. They only provide guidelines as directions to follow in search for a solution.

In the end, even though identification of the user is not a problem for an ISP technically, legally it is a complicated problem without a clear solution. Additionally, ISPs are greatly concerned with losing their clients (users) if they disclose their personal data to third parties.
2. EU LEGAL FRAMEWORK ON THE LIABILITY OF ISPs

2.1 Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-Commerce Directive)

2.1.1 The aim of the Directive 2000/31/EC

The reason for the enactment of the E-Commerce Directive, was the intention to use the advantages of Single Market and single currency to establish a new, digital dimension of the Single Market which was believed to “promote trade, stimulate innovation and competitiveness, create sustainable jobs and offer better quality of goods and services for lower prices”4. Hence, the European Union wanted to take full advantage of unique commercial possibilities and by enacting this Directive it gave the operators, the ISPs, legal certainty to operate their business and digital services without interruption or excessive obligations.

Main objective of this Directive is to remove legal barriers and enable free movement of informational society services which would facilitate online transactions as a major asset of internal market5, hence the provisions dealing with the liability of ISPs and the exemptions thereof are the tools needed to achieve such objectives.

The transactions which were going through ISPs’ services also included transactions of intangible property such as copyright. Issues arose once transactions of these goods were performed without authorization of the right holders, which is necessary for legal transaction. The right holders wanted to protect their rights and turned to ISPs as the ones in the best technical position to terminate the infringements.

The exemptions from liability are rebuttable presumptions if all conditions are met and do not need judicial involvement to be established, therefore serve as a ‘shield’ for ISPs to provide information services on a consistent base.

---

Exemptions from liability

2.1.2 Mere conduit (Article 12 of the E-Commerce Directive)

In instances when ISP provides transmission as an automatic transfer of data which is stored for a limited period of time necessary to complete the transmission, and if the ISP is not actively and intentionally involved in the transmission, the ISP shall enjoy immunity, even if the data transferred is copyright infringing.

In order for an ISP not to be considered actively and intentionally involved in the transmissions, the ISP must not:

a. Initiate transmission,
b. Select the receiver of the transmission,
c. Select or alter transmitted information.\(^6\)

This provision is important especially when copyright infringement has been performed through P2P file sharing, as ISP has enabled the connection between two peers. In these situations right holders cannot hold ISPs liable as they were not actively involved in the transmission, they only connected ‘peers’. Knowledge does not play an important role here unlike in Articles 13 and 14, as ISPs should not have any. The moment ISPs acquire any knowledge of the content transmitted through their services, they can no longer enjoy the immunity as this knowledge proves that there has been more involvement than ‘mere conduit’.

2.1.3 Caching (Article 13 of the E-Commerce Directive)

Caching is an act of storing data in cache (a type of temporary computer memory). This act is performed when data is accessed for the first time. If the same data is requested later on, the browser will get it from the cache, and not from the original server. This is done for the user’s convenience as it allows faster response and disburdens internet traffic.

---

\(^6\) Article 12(2) of the Directive 2000/31/EC on Electronic Commerce
Occasionally, the data stored in cache is condemned as infringing and in case of caching as automatic, intermediate and temporary storage, an ISP will not be liable for the infringement if the sole purpose of the storage was to efficiently facilitate onward transmission and given that the ISP:

a. does not alter cached data,
b. complies with the condition on access to the data,
c. regularly updates and monitors the data stored in cache in a manner widely recognised and used by the industry.

In instances when data is requested, the browser will show data previously stored in cache, which might not be up to date with data found on the original server. In order to avoid saving the infringing content even in cache, the ISP should regularly update and remove the data from cache memory, which can no longer be found at the original source.

d. lawfully uses the technology, recognised and commonly used by industry, to obtain data on the use of information,

e. acts expeditiously to remove or disable access to cached data if actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network or access to it has been disabled, or that the court or administrative authority has ordered such action is acquired.7

In comparison to mere conduit, ISP does more in the sense that it temporarily stores data. Two obligations can be distinguished here, initially an ISP should not interfere with the data as in the mere conduit provision, unless it acquires ‘actual knowledge’ which triggers an obligation to remove or restrict access to it.

Article 13(2)(e) presents an issue regarding the meaning of the term ‘actual knowledge’. The Directive does not provide the definition of this term and courts have had trouble defining it. This also creates legal uncertainty for ISPs and right holders, as ISPs are not sure when they have gathered enough knowledge to act and right holders are not certain if they have provided enough information for ISPs to acquire ‘actual knowledge’.

7 Article 13(1) of the Directive 2000/31/EC on Electronic Commerce
Steps to define it in more detail were taken within national laws, although this was not uniformly done and has led to defragmented interpretation of the term ‘actual knowledge’.\(^8\)

2.1.4 Hosting (Article 14 of the E-Commerce Directive)

Hosting is a type of service where ISPs provide their customers with space on a server to publish content. An ISP will not be liable for the infringing content stored at the request of a recipient if it:

a. “Does not have actual knowledge of illegal activity or information and as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent.”\(^9\)

Here, the Directive makes a distinction: to be held liable, an ISP has to have an ‘actual knowledge’, while for the damages it is sufficient that they have a constructive knowledge of the surrounding circumstances.

b. Obtains such knowledge or awareness and acts expeditiously to remove or disable access.\(^10\)

Even though hosting someone else’s content is still a passive role for an ISP, the Directive imposes “duties of care, which can reasonably be expected from [ISPs]”\(^11\). This comes close to the common law ‘strict liability’ theory. Even though an ISP did not infringe IPRs, the ISP provided services which were used by a third party to infringe IPRs. As this is a common practice known to ISPs, they are expected to exercise duties of care to prevent these actions or expeditiously terminate them. If the duty of care has not been shown, even

\(^8\) For further reference see Spanish Supreme Court cases SGAE v. Asociación of Internautas and Quejasonline case. “Spanish law has given definition of when ISP have actual knowledge a) That there is a prior decision, either by a court or by an administrative body, b) That the copyright infringement is voluntarily recognized, c) Other measures that may be established – this is the problematic part. Does this mean there will be further legislation that will define “other measures” (strict or closed interpretation) or does this include any other form of acquiring knowledge (open interpretation)”. For further reference see Peguera Miquel, “Internet Service Providers’ Liability in Spain Recent Case Law and Future Perspectives” available at https://www.jipitec.eu/issues/jipitec-1-3-2010/2823/peguera-isp-liability-spain.pdf, last accessed on 30.01.2018.

\(^9\) Article 14(1) (a) of the Directive on electronic commerce 2000/31/EC

\(^10\) Article 14 (1) (b), ibid

\(^11\) Recital 48, ibid
though there is no direct correlation between the ISP and the infringement, the ISP will be considered liable due to negligence or omission.

In instances when ISPs host their own content indirectly through the recipient of the service who is acting under the authority or the control of the ISP\textsuperscript{12}, there is no ground for immunity on the basis of this Article.

Hosts can exercise different levels of influence on the hosted content. Hosts which “have a greater influence on and control over the websites than traditional hosting providers, it is generally assumed to [...] also have a broader duty of care to ensure that their sites and platforms remain free of infringing material”\textsuperscript{13}. Consequently, they should constantly be on the lookout for the infringing material which is inconsistent with the Article 15 of E-Commerce Directive. This inconsistency is due to the absence of the ‘Good Samaritan’ clause which can be found in the CDA Section 230\textsuperscript{14}. If it had existed the ‘Good Samaritan’ clause would have enabled ISPs to check hosted material and voluntarily, in good faith, remove it without legal consequences.

2.1.5 Gaps and positive aspects

The E-Commerce Directive represents an EU version of the US DMCA ‘safe harbor’ provision and the CDA Section 230. With similar conditions, the main difference between the two systems lies in the procedure established by the DMCA for instances when an ISP has acquired knowledge about the existence of the infringing content (‘Notice and Take

\textsuperscript{12} Article 14(2), ibid
\textsuperscript{13} Sloot, Bart van der, “Welcome to the Jungle: The Liability of Internet Intermediaries for Privacy Violations in Europe” available at https://www.jipitec.eu/issues/jipitec-6-3-2015/4318, last accessed on 30.01.2018.
\textsuperscript{14} CDA Section 230 (c)
“Protection for ‘Good Samaritan’ blocking and screening of offensive material
(1)Treatment of publisher or speaker
No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
(2)Civil liability
No provider or user of an interactive computer service shall be held liable on account of—
(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1)”
Down procedure’). The DMCA provides a very detailed explanation of the procedure and notification forms, thereby eliminating a possibility of misinterpretation, which can be seen in Terms of Services of many platforms situated in the US such as YouTube, Facebook, and Instagram which simply copy the DMCA and CDA provisions.

Another significant gap left by the Directive is the lack of guidance for private notification procedure in relation to the infringing content existing on ISPs’ platform. As according to article 15 of the E-Commerce Directive, ISPs cannot constantly monitor transferred data, hence private notification procedure might be the most important and the effective way how ISPs would acquire knowledge of the infringing material. 15

A positive side of this Directive is that it has given a clear answer to whether Member States can impose obligations on ISPs to monitor the information which they transmit or store or actively seek facts or circumstances indicating illegal activity, as they provide services as mere conduit, caching and hosting. 16 A negative answer has confirmed that the EU clearly stood against mass-surveillance and acknowledged the difficulties and dangers thereof.

The E-Commerce Directive did not establish general liability, but rather exemptions therefrom. This is probably due to the differences existing in Member States’ copyright laws, especially concerning the exemptions and limitations regarding the legal use of copyright protected works, hence the formulation needed to be such so that it could be transposed into any legal framework.

However, the Directive has left space for national legislators to impose an obligation on ISPs to promptly inform competent authorities of alleged illegal actions or communicate the information which would enable identification of service recipient at their request. This meant that anti mass-surveillance attitude of the EU will not provide shelter for illegal acts including IPRs infringements. For this reason the Directive does allow for monitoring in specific cases. 17 Reviewed provisions granting immunity to ISPs imply that even if they will

16 Article 15(1) of the Directive on electronic commerce 2000/31/EC
17 Recital 47, ibid
not be held liable for copyright infringements, this would not stop authorities to order ISPs to take action to terminate or prevent future infringing acts.


The main disadvantage of all regulations regarding digital environment including ISPs liability, is that they have already been outdated at the moment of their endorsement. The pace of changes in digital environment is far swifter than any legal system can react to, and the continuous update is necessary. As “Digital Single Market strategy aims to create digital environment for the flourishing of online economy”\textsuperscript{18}, the Proposal attempted to resolve the rising issue of digital piracy by new regulation of ISPs’ liability in order to facilitate proper functioning of Single Market.

The Proposal introduces an obligation for ISPs which “store and provide access to the public to copyright-protected works uploaded by their users, thereby going beyond the mere provision of physical facilities and performing an act of communication to the public, to conclude licensing agreements with right holders, unless they are eligible for [hosting liability exemption]”\textsuperscript{19}. In addition, ISPs should “ensure the functioning of agreements concluded with right holders for the use of their works […] or to prevent the availability on their services of works”\textsuperscript{20}. To secure the enforcement of these agreements, the ISPs should employ the “use of effective content recognition technologies”\textsuperscript{21}.

Article 13, read in line with the recitals 38 and 39 of the Proposal, presents an innovative yet problematic solution. The issue arises as these provisions are not compatible with the existing EU legislation, specifically the E-Commerce Directive and CJEU case law. Recital 38 misinterprets communication to the public as “storing and providing access to

\textsuperscript{19} Recital 38 (1) Proposal for Directive on copyright in the Digital Single Market
\textsuperscript{20} Article 13 (1), ibid
\textsuperscript{21} ibid
the public of copyright-protected works” while E-Commerce Directive excludes ISPs’ liability for this act. According to the recital 38 hosting provider is “considered publisher, thus could be liable for all infringements of all laws that may be committed by their users even without actual knowledge” in instances when they “optimise the presentation of or promotion of the uploaded works or other subject matter” as this “goes beyond action of mere provision of physical facilities and performing an act of communication to the public”. In addition to being contrary to the wording of the existing legislation and Sabam v Netlog case, this change would have a “ ‘chilling effect’ on freedom of expression, and a massive private censorship, undermining innovation and competition”, amplifying the pre-existing issues.

The Proposal specifically chose CRT as an efficient, appropriate and proportionate measure to ensure enforcement of concluded agreements. CRT requires constant monitoring of all data passing through ISP’s service, thus imposing a general monitoring obligation prohibited by Article 15 of E-Commerce Directive. Additionally, the CJEU confirmed in the Netlog case, that such filtering systems do not strike a fair balance among fundamental rights as they cannot recognise legal uses of copyright protected works (parody, reviews, etc.). It is also not advisable for a legislation to tie itself to one specific technology as the rapid evolvement of such technologies would make the provision outdated.

As a conclusion, the EU has taken steps to update the existing legislation in accordance with technical developments and has also recognised the benefits of technology.

---

22 “Updated position paper: Article 13 remains a terrible idea and needs to be deleted” available at https://www.communia-association.org/2017/09/14/updated-position-paper-article-13-remains-terrible-idea-needs-deleted/, last accessed on 30.01.2018.
24 Recital 38 (2) of the Proposal for Directive on copyright in the Digital Single Market
25 Recital 38 (1), ibid
27 Article 13(1) of the Proposal for Directive on copyright in the Digital Single Market
in the battle against cyber piracy. However, any future development of the EU legal system should be in consistency with the existing legal system, especially the E-Commerce Directive, its wording and principles set up by the CJEU case law while taking into account the drawbacks of existing CRTs. Nevertheless, the proposal did leave space for future improvement in the form of “notice-and-action system or a duty of care for intermediaries to remove notified content”29 (the ‘Good Samaritan’ clause).

3. EU LEGAL FRAMEWORK REGULATING THE HARMONIZATION OF COPYRIGHT AND RELATED RIGHTS AND THE ENFORCEMENT OF INTELLECTUAL PROPERTY RIGHTS

3.1 Harmonising copyright and related rights in the EU information society

Primarily, copyright right holders base their rights on national legislations which vary, from one country to another leading to defragmentation and preventing the free movement of goods and services across the Member States’ borders. The InfoSoc Directive\(^{30}\) took on the task to harmonise some aspects of copyright and related rights in order to make their ‘trade’ on the internal market easier, benefiting the creators as they would have access to a market wider than their national and, also benefiting the market itself as it would avoid problems regarding application of private international law. Directive was widely criticised as being written for main players (publishers, broadcasters) and not for the creators.\(^{31}\) Its objective is to establish and define rights, while the Enforcement Directive contains provisions dealing with their implementation and enforcement.

The InfoSoc Directive provides a reasoning as to why a uniform liability of ISPs towards copyright protected content is still aim out of reach. The InfoSoc has established exceptions and limitations allowing legal use of copyright works without authorisations and/or a fee. Each Member State can choose which of the exceptions and limitations to transpose into national legislation, which implies that what is considered a legal use in one country does not necessarily mean that it would be a legal use in another as the States may have not transposed the same exception or limitation from the InfoSoc Directive. Due to these conditions it is not possible to pass legislation at an EU level which would definitively state which content should be blocked or removed by ISPs as infringing.

However, in Article 8 (3) it did provide for a ‘tool’ to right holders to combat online infringements by allowing injunctions against ISPs whose services were used by a third party

---

\(^{30}\) Directive 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society

to infringe their rights regardless of ISPs’ liability. Further specifications are left to each Member State due to procedural differences, with an aim for injunctions to be effective, proportional to the infringing action and circumstances, and dissuasive for further infringements. Even though the Directive stands for a “rigorous, effective system for the protection of copyright”\(^\text{32}\) its provisions “shall be without prejudice to provision regarding [...] security, confidentiality, data protection and privacy”\(^\text{33}\), meaning it omitted to regulate if ISPs should disclose user’s personal data for the purpose of court proceedings.

3.2 Enforcing IPRs in the digital environment

Due to the flourishing of digital piracy, the ‘offline’ EU enforcement legislation was unable to deliver the needed effect. Passing of the Enforcement Directive\(^\text{34}\) was not supported by great political enthusiasm, although it was needed. It integrated provisions of TRIPS Agreement, providing minimum rights for right holders at the EU level while allowing Member States to grant preferable status. Due to the unfavourable political environment some “provisions, notably those that go beyond TRIPs Agreement were limited to infringement of IPRs committed on a commercial scale or causing significant harm to the right holder”\(^\text{35}\) and to claims for IPRs infringements in civil proceedings\(^\text{36}\).

The Enforcement Directive seems to be an elaboration of the Article 8 of InfoSoc Directive. It has repeated the same aim of ‘effective, proportional and dissuasive’ measures, procedures and remedies by obligating Member States to “provide for the measures, procedures and remedies necessary to ensure the enforcement of IPRs covered by it”\(^\text{37}\).

---


\(^{33}\) Article 9, ibid

\(^{34}\) Directive 2004/48/EC on the enforcement of intellectual property rights


\(^{36}\) The Enforcement Directive focuses on civil proceedings and civil sanctions. It has left out criminal sanctions, as they proved to be too big of an obstacle in the process of negotiation and were later introduced in a separate Amended proposal for Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights known as IPRED 2.

\(^{37}\) Article 3(1) of the Directive 2004/48/EC on enforcement of IPR
For the right holders, Article 11(3) is the most important, obligating Member States to “ensure that right holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe”\textsuperscript{38} their copyright regardless of the ISPs’ liability. This provision intended to ease the resistance of ISPs towards the implementation of injunctions. They will not be held liable for the infringement committed by their users, however, they will have to act to stop it. Injunctions against ISPs may consist of taking down the infringing material, which could satisfy right holders as their work would no longer be publicly available and they would not have to initiate a complicated procedure to identify and prosecute the person who uploaded it.

Additionally, Article 8 imposes an obligation to Member States to ensure that judicial authorities can upon proportional and justified request by right holders order ISPs to disclose information on the origin of the services infringing copyright, as they are “found to be providing on a commercial scale services used in the infringing activities”\textsuperscript{39}. These provisions should have been the ‘golden ticket’ for right holders, however they did not bring about such effect. Even though, it is an obligation of the State, a court has the freedom to decide whether to order information disclosure, thereby lessening the impact of these provisions. States and their judicial authorities have been greatly reluctant to deliver such decisions due to the lack of indications specifying when the request of the right holder will be considered ‘justified and proportional’ to order disclosure of personal data.

Along with the InfoSoc Directive, the Enforcement Directive represents cornerstone of the battle against piracy in cyberspace. It can be noted that the Enforcement Directive has tilted the balance in favour of the right holders, by allowing courts to order disclosure of data regarding users using ISPs’ services for infringing acts. On the other hand, it did not provide answers to the status of ISPs in such situations.

\textsuperscript{38} Article 11(3) of the Directive 2004/48/EC on enforcement of IPR

\textsuperscript{39} Article 8 (1) (c), ibid
4. EU LEGAL FRAMEWORK REGULATING THE PROTECTION OF PRIVACY AND PROCESSING OF PERSONAL DATA

4.1 Protection of individuals in the processing of personal data

Privacy and protection of personal data represent one of the main obstacles in the enforcement of copyright in digital cyberspace. As the date states, the Directive 95/46 was enacted long before digital piracy gained such influence on the internal market, therefore some of its provisions are not tailor made for online environment. It has provided a starting point from which more appropriate directives have been developed and it is being continually revised by the Article 29 Working Party.

The aim of the Directive is to preserve anonymity on the Internet, in the sense that users do not have to reveal their personal data when this is not necessary, in order to access certain information services. The Directive also introduced ‘the minimality principle’ which prohibits the collection of data without a specific purpose and for the duration longer than is necessary.40

The importance of this directive in the battle against digital piracy increased after the CJEU decision in Breyer41 case confirmed that dynamic IP address is personal data, and therefore enjoys all privileges and protection under this Directive. An IP address per se cannot identify an individual, but when combined with other data in possession of ISPs, it can point to a single person.

The Working Party is of the opinion that databases of personal data may be used only for the purpose they were created for. As ISPs have databases of users’ personal data for the purpose of providing telecommunication services, it would not be legal for them to use the databases in order to facilitate court proceedings. 42

---

40 Article 6 of the Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
41 The CJEU case Patrick Breyer v Bundesrepublik Deutschland C-582/14
However, Directive 95/46 introduced exemptions which allowed Member States to adopt legislation restricting the protection provided by the Directive. What is particularly important for the topic of ISPs’ secondary liability is that one of the reasons for restriction is “the protection of the data subject or of the rights and freedoms of others.”

There are two interpretations of this provision. According to the first interpretation, Member States can adopt legislation which allows ISPs to make available to the third party (the right holder of the infringed copyright) user’s personal data as the right to property of the third party has to be protected. The second interpretation reflects on Recital 30, which states that “the data can be processed in the legitimate interest of a natural or legal person if the rights and freedoms of the data subject are not overriding.” The Directive itself has not given a clear answer if piracy would be perceived as sufficient to overrule the protection of privacy. It has however allowed Member States to make such decisions for themselves.

In order to solve the problem of digital piracy, without infringing the right to privacy or turning ISPs into copyright police, Article 29 Working Party has called for the development of technologies which would a priori prevent infringements and in cases where an investigation is carried out by private actors such as copyright holders or their representatives, for it to be strictly in a clear legal framework along the established principles.

43 Restricting the scope of articles: Article 6.1. - principle relating to data quality, Article 10.-Information in cases when data is collected from data subject, Article 11.1.information when data is not collected from data subject, Article 12 – right of access, Article 21.- publicizing of processing operations; Directive 95/46
44 Article 13(1)(g) of the Directive 95/46
45 Recital 30, ibid
4.2 Processing of personal data and the protection of privacy in the electronic communications sector

An updated version of the Directive 95/46 is the Directive on privacy and electronic communications with an objective to harmonise the protection of fundamental rights and freedoms, primarily the right to privacy and secrecy of communication in the electronic communications sector. The Directive intended to raise the standard of privacy protection in electronic communications by proactively engaging users by allowing them to exercise their privacy choices. This was done by introducing an ‘opt-in’ cookie policy, in the sense that users first need to give their consent and only then the data can be stored and processed, contrary to the pre-existing ‘opt-out’ cookie policy.

As publicly available communication services present a new danger for personal data and privacy the Directive imposes an obligation on ISPs to take measures to safeguard the security of their services. This consists of informing subscribers of possible dangers, how to avoid them and if any new unforeseen risks arise, it is ISP’s obligation to resolve it at their own cost. 

Article 3 restricts the scope of the Directive to only publicly available communication services. This is considered to be limiting and amendment has been made to include private communication services which are intentionally open for public access. However, this was not changed even with the Directive 2009/136.

---

Even though the aim of the Directive was to upgrade privacy protection by prohibiting surveillance or interception of communication, Article 15 allowed Member States to adopt legislation that may restrict guaranteed privacy of communication when they find it to be necessary, appropriate and proportionate within a democratic society. As one of the reasons for the restriction is mentioned in the Article 13 of the Directive 95/46, which allows for the restriction to the protection provided that the rights and freedoms of others have to be protected. In a sense, the Directive has modernized, but also repeated the same mistake as the Directive 95/46, giving no guidance as to which rights and freedoms could repeal the protection of private data.

4.3 General Data Protection

As a step in the process of legal innovation, EU enacted the General Data Protection Regulation which “replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens’ data privacy and reshape the way organizations across the region approach data privacy”54. GDPR aims to award constant protection to natural persons with regard to the processing of personal data and the rules relating to the free movement of personal data55 in a “data-driven world”56. The GDPR is applicable regardless of the technology used for the processing of personal data (non-automated or automated), “assuring that protection afforded by the GDPR is not circumvented through the use of various techniques”57.

While GDPR is awaiting its enforcement in May 2018, it has already initiated debates. GDPR strives to find a balance between the right to privacy and the right to information; however, it does tilt the balance in favour of privacy which can clearly be seen in the ‘Notice and Take Down procedure’. This procedure is used to enforce the right to be

54 “GDPR Key Changes” available at https://www.eugdpr.org/eugdpr.org.html, last accessed on 30.01.2018.
55 Recital 12 GDPR 2016/679
forgotten (right to erasure)\textsuperscript{58}, allowing data subjects to request that their personal data available online be erased, ceased from future dissemination or to halt processing by third parties, under certain conditions.\textsuperscript{59} The aim of the procedure is to facilitate the removal of personal data in order to secure privacy and prevent the misuse of personal data.

‘Notice and Take Down procedure’ is important for ISPs which host third party content as it allows them, upon receiving a clear request, to temporarily remove the content and investigate the infringement afterwards. If the claim for removal is valid, the content will be permanently removed, otherwise the content may be re-published. In addition, a subject requesting the removal has the right to ask an ISP to disclose the information regarding the user who posted the removed content.\textsuperscript{60} Furthermore, the ISP does not have to inform the user that his post has been removed. Consequently, these provisions have initiated a debate on whether there is a balance of rights at all in the silent content removal procedure. Likewise, it is sometimes challenging to understand the GDPR’s relation to the existing directives, especially E-Commerce Directive, as it remains unclear which of them will guide the process of ‘Notice and Take Down’. \textsuperscript{61}

The procedure enacted by GDPR, even though not directly connected to copyright, was recognized by copyright right holders as a model which could be used to remove the infringing content in a similar manner as it removes the personal data available online. Therefore a question emerges: Can the procedure ‘Notice and Take Down’ which removes first and investigates later, be considered as respectful to the balance of fundamental rights referred to by the CJEU in Promusicae case\textsuperscript{62}? It is a personal opinion of the author that such procedure would create a large-scale and ‘silent’ censorship, as one would not be informed about their content removal or of reasons thereof, which may cause more harm than good. Presumption of innocence in this situation would work in reverse since one

\textsuperscript{58} Article 17 of the GDPR
\textsuperscript{59} “GDPR Key Changes: An overview of the main changes under GPDR and how they differ from the previous directive” available at https://www.eugdpr.org/key-changes.html, last accessed on 30.01.2018.
\textsuperscript{61} Ibid, pp. 60-71
\textsuperscript{62} Productore de musica de Esana (Promusicae) v Telefonica de Espana (C 275/06)
would first be proclaimed an infringer and then if the infringer initiates a proceeding, the opposite could be proved. This procedure, preferred by ISPs and right holders, makes freedom of expression and right to receive and impart information an easy target, which is not acceptable.
5. CJEU CASE LAW

5.1 Searching for a balance between fundamental rights through the case Productore de musica de Espana (Promusicae) v Telefonica de Espana (C 275/06)

5.1.1 Background information and the issue

Promusicae, Spanish non-profit organisation representing music producers, claimed that it identified a number of IP addresses which were used for peer-to-peer file sharing (using KaZaA file exchange program) specifically music files, in which its members have copyright and have not authorized it. In order to bring civil proceedings against infringers, Promusicae had to identify them, and therefore requested from Telefonica as the ISP to disclose the identities and addresses, correlating with particular IP addresses. Telefonica refused to do so, citing that Article 12 of the Spanish LLSI interpreted in the light of Directives 2001/31, 2001/29, and 2004/48 allows disclosure only in cases of criminal investigation, safeguarding public security and national defence, while Promusicae believed that said article should be interpreted in a broader sense so to include copyright infringement. The Spanish Appellate Court stayed the proceedings and referred the question to the CJEU asking if the above mentioned directives required “Member States to lay down, in order to ensure effective protection of copyright, an obligation to communicate personal data in the context of civil proceedings”?

5.1.2 Court ruling and effect on liability of ISPs

The aim of the directives mentioned by the Spanish court is to provide effective protection of copyright, “however this [...] does not prevail over the protection afforded to

---

63 Opinion of Advocate General Kokott regarding case Promusicae v Telefónica (C-275/06) from 18.07.2007.
65 Paragraph 41 of the Court decision Promusicae v Telefónica (C-275/06)
personal data by Directives 95/46 and 2002/58. On the other side, according to the Enforcement Directive judicial authorities upon justified and proportional request may order to ISPs, as they are providing telecommunication services on a commercial scale which are used to infringe copyright, to disclose information of the origin of the service infringing copyright. In addition InfoSoc Directive allows “injunctions against ISPs whose services are used by a third party to infringe copyright” and the Charter of Fundamental Rights of the EU, states that right holders have the right to protect intangible property and the right to an effective remedy.

The issue of the case in question is of fundamental rights - equally important and protected- opposing each other.

The Court responded that these provisions had to be read in conjunction with acquis communautaire in order to comprehend their true meaning. Having in mind the EU legal system as a whole and the language of the referred Directives, the Court could not find that acquis communautaire orders Member States to allow disclosure of personal data for the purpose of civil proceedings. Additionally, provisions 41, 42, and 47 of the TRIPS Agreement do not state that disclosure of personal data is necessary for effective protection of copyright. Article 47 of the TRIPS Agreement only gives an option that Member States may do so if they find it to be necessary.

In the opinion of the CJEU, the only way to solve this gridlock is to find a balance among these fundamental rights. A mechanism to find the balance can be found first, in the Directive 2002/58 which provides exceptions from confidentiality of personal data, second in the directives referred to by national court which coordinate rights regulated by those directives and the protection of privacy, and third in the specific circumstances of the case. When implementing measures from transposed directives the authorities should interpret

---

67 Article 8(1) of the Directive 2004/48 on the enforcement of IPR
68 Article 8(3) of the InfoSoc Directive 2001/29
69 Article 17- Right to property and article 47 – right to an efficient remedy and fair trail, Charter of the fundamental right of the EU
71 Paragraph 66 of the Court decision Promusciae v Telefonica (C-275/06)
them in a manner consistent with national law and general principles and fundamental rights of the Community.  

In conclusion, the national court would have preferred a clear answer to where a ‘fair balance’ of fundamental rights is, while the CJEU referred it back to the national court without specific guidelines. For ISPs it meant no obligation to disclose their users’ personal data unless a Member State finds it necessary due to” their own judgment as to what sits well with their socio-legal and economic tradition”\textsuperscript{73}. Unfortunately this has given ISPs no legal certainty, as some will be obliged to disclose the information regarding their users, while others in similar cases but in different Member States will not.

5.2 Providing access to the Internet is enough to constitute ISP’s secondary liability in the case \textit{LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH (C-557/07)}

5.2.1 Background information and the issues

LSG is an Austrian collecting society representing performers and phonogram producers which, requested Tele2 as an ISP to reveal the names and addresses of their users whose IP addresses were found to infringe related rights. Tele2 denied this request claiming that it was not an intermediary within the meaning of Article 8(3) of the InfoSoc Directive and that they do not store trafficking data.\textsuperscript{74} Austrian Supreme Court had to stay the proceeding and referred two questions. The first question was if “an access provider, which only provides its users with access to the Internet without any other services [such as email, FTP or file-sharing services] and without exercising any control, \textit{de iure or de facto}, could be considered as an intermediary within the meaning of Articles 5(1)(a) and 8(3) of

\textsuperscript{72} Paragraph 70 of the Court decision Promusicae v Telefonica (C-275/06)

\textsuperscript{73} Stamatoudi Irini, “The role of Internet Service Providers, Ethics, Reality and the Law: \textit{The Example of Promusicae v. Telefonica}”, in “\textit{Computer Ethics: Philosophical Enquiry}” by Maria Bottis (ed.) from 8th International Conference Corfu 26-28 June 2009, Ionio University, Nomiki Vivliothiki (2009), Athens, pp. 750-767

Directives 2001/29? The second question similar to the one in Promusicae case was whether the EU law “precludes Member States from imposing an obligation to disclose to private third parties personal data relating to Internet traffic in order to enable them to bring civil proceedings for copyright infringements”.

5.2.2 Court ruling and effect on liability of ISPs

The InfoSoc Directive asks Member States “to ensure that right holder are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe [their right].” Tele2 was providing a service which was sufficient to infringe copyright by a third party, hence such providers will be considered as an intermediaries within the meaning of Articles 5(1) (a) and 8(3) of Directive 2001/29. An opinion contrary to this would narrow down the application of the InfoSoc Directive by excluding a large number of ISPs and severely compromising right holders’ ability to apply for injunctions and enforce them. This ruling has made clear for ISPs that from the moment of providing Internet connection to users, even if they do not exercise any control over it, they could be held secondary liable for copyright infringements committed by their users.

As for the second question, the CJEU repeated the ruling from the Promusicae case stating that it was up to each Member State to decide whether to allow ISPs to disclose users’ personal data for the purpose of civil proceedings if they believed it to be suitable to achieve intended objective, necessary as it is the least restrictive measure capable to achieve the result and proportional stricto sensu meaning the result pursued compared with the consequence to the fundamental rights is in balance.

---

75 Paragraph 30 of the court decision LSG V TELE2 (C-557/07)
76 Paragraph 24, ibid
77 Article 8(3) Directive 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society
5.3 Confirming prohibition of obligation of general monitoring by ISPs in the case
Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)
(C-70/10)

5.3.1 Background information and the issue

The case was originally brought before the Belgian Court when SABAM, a collecting organisation representing authors, composers and publishers brought interlocutory proceedings against ISP Scarlet as it had knowledge that Scarlet’s services were used for P2P file sharing of copyright-protected works from the SABAM repertoire. SABAM proposed to the court to install filtering and blocking systems which would overview all P2P traffic and search for copyright-protected works. During the proceeding, the court appointed an expert who concluded that out of eleven filtering systems SABAM proposed, seven were applicable to Scarlet’s network in order to recognise and block targeted files.\(^{80}\) The Brussels Court of First Instance found SABAM’s request legitimate and ordered Scarlet to disable unauthorised communication of copyright-protected works to its users. Consequently, Scarlet appealed stating that the first instance judgment was directly in conflict with Article 15 of the E-Commerce Directive. Therefore, the Court of Appeal stayed the proceeding and referred a question to the CJEU asking if it was consistent with the EU law and the European Convention on the Protection of Human Rights and Fundamental Freedoms for Member States to allow national courts “before which substantive proceedings have been brought […] to order an [ISP] to install, for all its customers, in abstracto and as a preventive measure, exclusively at the cost of that ISP and for an unlimited period, a system for filtering all electronic communications, both incoming and outgoing, passing via its services, in particular those involving the use of peer-to-peer software, in order to identify on its network the movement of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold rights, and subsequently to block

\(^{80}\) Paragraph 21 and 22 of the Court decision Scarlet v Sabam (C-70/10)
the transfer of such files, either at the point at which they are requested or at which they are sent.”

5.3.2 Court ruling and effect on liability of ISPs

The Court was of the opinion that the preventive measure requested by SABAM did not ensure balance between competing fundamental rights including ISP’s freedom to conduct business. Such filtering systems would not be able to distinguish authorised and infringing use of works, thereby affecting users’ freedom to receive or impart information. From the standpoint of ISP, such injunction imposes new costs, new obligation to monitor communication and a new role, online copyright policing which could affect their freedom to conduct business. The only winner would be the copyright indicating imbalance among these fundamental rights.

Article 15 of the E-Commerce Directive prohibits national authorities from adopting measures which would require an ISP to carry out general monitoring of the information that it transmits on its network, thus courts of the Member States will not be able to issue injunctions with no geographical, durational or qualitative limits as they are not found to be necessary, effective and proportionate as requested by Article 8 of the InfoSoc Directive and Article 3 of Directive 2004/48.

The CJEU reaffirmed neutral role of ISPs, which would enjoy immunity with certain exceptions. However, this is not a definitive ‘no’ to filtering and blocking systems. We will have to see what will happen if more precise and sophisticated filtering systems emerge in the future.

---

81 Paragraph 28(1) of the Court decision Scarlet v Sabam (C-70/10)
5.4 Additional prohibition of general monitoring obligation by hosting providers in the case Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV (C 360/10)

5.4.1 Background information and the issue

This is another case initiated by SABAM however, this time against Netlog (now a part of the Twoo), a social networking platform which allowed its users to create profiles to meet people. Users of this platform could also share photos and videos and some of the shared files were copyright-protected works whose right holders were represented by SABAM. Therefore, SABAM initially approached Netlog asking for a compensation for unauthorised use of the protected works by its users, but Netlog refused this proposal, which led to the court proceeding.

Although there are similarities with the case SABAM v Scarlet, the defendant in this case is a social networking platform acting as a host which stored information provided by users on its servers, while Scarlet was an ISP which provided access to the Internet, but did not store users’ information, with the exception of cache memory. The question referred was the same as in the SABAM v Scarlet case, was it possible for a court to order ISPs to install general, permanent filtering system.

5.4.2 Court ruling and effects on the liability of ISPs

The ruling was in consistency with SABAM v Scarlet case, confirming that filtering systems without geographical, durational and qualitative limitations may not be imposed as an obligation onto ISPs, even though in this case Netlog was storing the infringing content

---

84 Within the meaning of Article 14 E-commerce Directive
86 Question referred: Can Member States allow national courts to issue injunctions against host whose services are used by a third party to infringe copyright by ordering ins “for all its customers, in abstracto and as a preventive measure, at its own cost and for an unlimited period, to introduce a system for filtering most of the information which is stored on its servers in order to identify on its servers electronic files containing musical, cinematographic or audio-visual work in respect of which SABAM claims to hold rights, and subsequently to block the exchange of such files?”, paragraph 25 of the Court decision SABAM v Netlog C-360/10,
in cache memory. Injunctions against intermediaries are the right of right holders; however the protection of copyright is not absolute as stated in Promusicae case and it ought to be found with respect to the balance of other fundamental rights.

The filtering system described in the referred question would be contrary to Article 15 of the Enforcement Directive and fundamental rights, as Netlog was storing data provided by users and such filtering system would have resulted in infringement of users’ right to privacy and the protection of personal data. Additionally, as current filtering systems are not able to distinguish between lawful and infringing uses, it would also impact the freedom of information protected by ECHR.87

Finally, ISPs are certain that regardless of their type and services they provide, they have no right to actively monitor services, as opposed to stopping an infringement, once they are aware of its existence.88

5.5 CJEU allows national court to adjudicate ‘open-textured’ remedies towards ISPs in the case UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH (Case C-314/12)

5.5.1 Background information and the issue

UPC Telekabel is a company providing Internet, telephone and TV services to its clients. Constantin Film and Wega are film production companies which have detected a website allowing unauthorized download and streaming of films to which they hold rights. They subsequently requested the UPC Telekabel to block access to the site in question, however, the UPC Telekabel refused on grounds that there was no contractual or business relationship between the UPC Telekabel and the operators of that particular site.

The Austrian court referred two questions to the CJEU regarding this case. The national court asked if ISPs could be considered as an intermediary within the meaning of

---

Article 8 (3) of the InfoSoc Directive, allowing right holders to apply for injunctions against ISPs as their services are used to infringe copyright, even if ISPs do not have business or contractual relationship between them and the site providing infringing content.  

The second question was if national courts could issue an injunction consistent with the EU law and fundamental rights, without specifying measures, which ought to be taken, and only stating the intended goal of blocking access to a protected subject matter available online, and if ISP could avoid incurring coercive penalties if they proved that they had taken all reasonable measures.

5.5.2 Court ruling and effects on the liability of ISPs

The CJEU held that Article 8(3) of the InfoSoc Directive does not require ISPs to be in any relation to the infringer for the right holders to be able to make an application for an injunction. A contrary interpretation would restrict the objective of the Directive, thereby excluding a large number of ISPs. In addition, the court provided an example, if UPC Telekabel was removed from the transmission, the download and streaming would be impossible, thus proving that UPC Telekabel is one of the key actors.

CJEU considered that any injunction issued by a court should aim to achieve the balance between the fundamental rights to property, privacy, freedom of information and business conduct. It has found that requiring ISPs to block access to a specific site hosting infringing content will not be considered disproportionate burden. The Court highlighted than any measure chosen should “be sufficiently effective to ensure genuine protection or

---

89 The question referred to the CJEU was if “Article 8(3) of Directive 2001/29 must be interpreted as meaning that a person who makes protected subject-matter available to the public on a website without the agreement of the rightholder, for the purpose of Article 3(2) of that directive, is using the services of the internet service provider of the persons accessing that subject-matter, which is to be regarded as an intermediary within the meaning of Article 8(3) of Directive 2001/29?” – paragraph 23 of the Court decision UPC Telekabel v Constatnin Film C 314/12
90 Paragraph 42, ibid
91 Paragraph 32, Ibid
at least making it difficult to achieve and seriously discouraging internet users to attempt infringing acts.”

Additionally, unspecified injunctions prohibiting certain outcomes will be more suitable for ISPs as they would allow them to determine which technical measures are applicable in a particular case while not exposing them to ‘unreasonable sacrifice’. ISP can choose from varieties of technical measures such as blocking domain name, IP addresses, URLs, de-listing from search index and other hybrid methods. They differ in costs, effectiveness, and promptness of implementation.

Advocate General was of the opposite opinion that ‘open-textured’ injunctions without further specifications, impose a difficult burden on ISPs in terms of how to balance the fundamental rights at stake. ISPs seek guidance from courts, as they have no definitive way to know if the measures implemented would be considered reasonable and fair unless being brought before the court once again. If an ISP overprotects copyright it will infringe freedom of information; and if it neglects it, it will be held secondary liable. This may lead to a perplexing situation. According to Article 15 of the E-Commerce Directive, a court cannot impose injunction of general surveillance. What will happen if a court issues an ‘open-textured’ injunction and ISP finds that filtering software is the most suitable in the particular case?

For ISPs this ruling was bittersweet. It has given them freedom and flexibility to choose mechanisms to terminate and prevent infringements, and through these measures they will have to find a balance among the fundamental rights, which is a task challenging even for the CJEU.

---


95 Eleonora Rosati, “CJEU says that blocking orders are OK and do not have to be specific” available at http://ipkitten.blogspot.rs/2014/03/breaking-news-cjeu-says-that-blocking.html , last accessed on 30.01.2018.
5.6 Extending the reach of awarded injunctions to future infringements through the case L’Oréal SA and others v eBay International AG and Others (324/09)

5.6.1 Background information and the issue

L’Oréal brought this proceeding against eBay and several of its users before the UK High Court of Justice, Chancery Division. L’Oréal claimed that eBay users infringed trademarks owned by L’Oréal by selling counterfeit products, samples provided to distributors free of charge, unboxed products, and non-EEA products on eBay and that eBay directed customers (buyers) once they typed keywords corresponding to the names of L’Oréal’s trademarks to counterfeited goods which were offered for sale on eBay. 96 The question referred to the CJEU asked for clarification regarding injunctions specified in Article 11 of Enforcement Directive. Do these injunctions oblige intermediaries to also prevent future infringements of IPRs, and not only to terminate the continuation of the current one?97

5.6.2 Court ruling and effects on the liability of ISPs

This question was referred as Article 11 of the Enforcement Directive does not give further details regarding the nature of injunctions and requires Member States to determine procedures and conditions for ordering injunctions, as well as methods applicable and their duration, all due to variations existing in civil and procedural laws among the Member States. However, some Member States have directly transposed Article 11 into national laws without further specifications.

The Court ruled that the correct interpretation of Article 11 of the Enforcement Directive was that “national courts with jurisdiction in relation to the protection of

97Referred question: " Where the services of an intermediary such as an operator of a website have been used by a third party to infringe a registered trademark, does Article 11 of [Directive 2004/48] require Member States to ensure that the trademark proprietor can obtain an injunction against the intermediary to prevent further infringements of the said trade mark, as opposed to continuation of that specific act of infringement, and if so what is the scope of the injunction that shall be made available?" - paragraph 50 of the Court decision L’Oréal v eBay (324/09)
intellectual property rights are able to order the operator of an online marketplace to take measures which contribute, not only to bringing to an end infringements of those rights by users of that marketplace, but also to preventing further infringements of that kind."98.

For ISPs, this meant that if right holders requested an injunction, that injunction obligated ISPs to terminate the existing copyright infringing acts and take necessary measures to prevent future infringements of the same copyright. How this will be executed as ISPs are not allowed to actively seek acts or circumstances indicating illegal activity nor they can impose general filtering systems ‘hunting’ for specific files, is yet to be seen.

---

98 Paragraph 144 of the Court decision L’Oréal v eBay (324/09)
6. MECHANISMS AGAINST ONLINE COPYRIGHT INFRINGEMENT

6.1 Law-based mechanism – the French HADOPI Law

A number of countries such as France have chosen to regulate the liability of ISPs for third party’s content through statutory regulations. There are several positive aspects to this mechanism. It ensures unified reaction by all ISPs, unlike the code of conduct which depends on the willingness of ISPs. Before the enactment, the law goes through a demanding and detailed procedure, with the aim to ensure that it was democratically debated by representatives chosen by the public. Additionally, its enforcement is governed by public authorities which gives a higher level of certainty that its aims shall be achieved.

A negative aspect of this mechanism is that the costs are usually high due to the complex procedure of enactment. Its complexity is also reflected in the time needed to enact such legislation. Unfortunately, cyberspace is a high-speed environment, where changes are common, making this mechanism always late in its reaction. This topic is highly technical hence the lack of specific knowledge among public representatives may limit their understanding of the problem and possible solutions.

In the case of France, prior to HADOPI law, several statutory regulations were enacted establishing a legal environment in which HADOPI could achieve its aims. Among those laws was the Data Privacy Law, allowing entities representing right holders to collect and process personal data in order to enforce copyright and Intellectual Property Code which obliged users to ensure that their Internet connections are not used for infringing activities.

The HADOPI legislation created a two-stage response system to online copyright infringements. It established HADOPI, an administrative authority, which “reviews alleged
instances of copyright infringements [received from sworn agents] and checks whether copyright ownership can be confirmed. Individual right holders cannot bring the facts directly to HADOPI. They have to be represented by a collecting society or ask the Prosecutor to indicate a procedure, to ensure that individual right holders may never have access to IP addresses or correlating personal data. By authorisation of the Data Privacy Law, HADOPI can request ISPs to disclose personal data on the basis of the IP addresses provided by sworn agents. As a result, the right holders do not have direct access to personal data correlating to an IP address, therefore secrecy of personal data is ensured while the prosecution of infringers is enabled.

In its first, educational stage, the ISPs shall notify the subscriber that his connection has been used for infringing activities, only providing the date and time of the infringement without disclosing the work that has allegedly been infringed, and the contact information of HADOPI for further clarifications. Additionally, the notification contains information on legal provisions condemning this activity as illegal, on lawful ways to access copyright-protected works and an explanation of the negative effects of piracy. If HADOPI detects a new infringement from the same IP address within six months from the first notification, it will send a second notification by registered mail. At this point, the educational stage ends.

Although undervalued, the educational element of this procedure has great potential. Research has shown that 70% of users would stop infringement after the first warning and additional 16% after the second warning. The public is greatly unaware of the infringing nature of their own acts, which could be eliminated or minimised through education and raising awareness on the negative impact of digital piracy. On the long run, education would

---


reduce the widespread of digital piracy performed by private users, thus eliminating the need for their prosecution which would save time, money and disburden courts.\footnote{107}

In the next stage, if HADOPI detects an infringement from the same IP address within a year from the second notification, it will initiate a proceeding before a single judge who can award a fine or suspension of the Internet connection for the period from two months up to a year.\footnote{108}

Since its enactment, HADOPI has gone through some modifications. Initially, the decision regarding the suspension of the Internet connection was in the hands of HADOPI. However, French Constitutional Council was among the first to proclaim that Internet access is a fundamental right as it is rooted in the freedom of expression. As “no restrictions may be imposed on the fundamental rights and freedoms of end users, without a prior ruling by judicial authorities”\footnote{109}, the Parliament decided to authorise judicial authorities to decide on internet disconnection. After these modification, HADOPI remained authorised to send educational notifications, which altered the aim of the law to set up an automated procedure to expeditiously prosecute online piracy.\footnote{110}

For ISPs, HADOPI law has brought legal protection against lawsuits for indirect copyright infringements as long as they cooperate with HADOPI and copyright holders.\footnote{111} It saved them money and time which would be spent on setting up a system of their own to fight against infringements.\footnote{112} However, there will be expenses as ISPs will have to establish a system allowing them to identify users, send notifications, maintain the data retained, etc. These expenses will, in the end, be borne by users through increased fees. Time will show if such legislation will result in ISPs losing both clients and profit. If this happens legal
certainty provided by the law shall no longer be appealing to ISPs and a new mechanism shall be installed.

6.2 Soft law mechanism – Dutch ‘Notice and Take Down’ Code of Conduct

In the recent years, there has been a gradual shift from statutory copyright enforcement in cyberworld to self-imposed regulations. ISPs have established codes of conduct among themselves to cope with the rising problem of digital piracy. They established these rules either to substitute for the lack of statutory regulation or to complement the existing laws which provided objectives and basic principles. The former is an example of the pure self-regulation, which is nowadays rare while the latter is a form of co-regulation with public authorities. Pure self-regulation is not advisable as the formulation of the provisions is solely in the hands of private parties, giving no guarantees to fundamental principles and freedoms.113

E-Commerce Directive114, Enforcement Directive115 and Proposal for a Copyright Directive116 encourage self-regulation and so do states as it liberates them from a long and costly procedure of statutory enactment. As ISPs have expert knowledge regarding data traffic management, hence the agreed solutions and procedures are developed with a better understanding of technical possibilities. Norm-setting procedure is flexible and, on most occasions quicker and cost effective compared to parliamentary procedure. Due to the lack of formalities, codes are easily revised and amended, enabling prompt responses to changes. However, codes are usually agreed on by stakeholders such as ISPs and right holders. Public authority representatives may be involved occasionally, while users are not represented at all which questions the democratic nature and transparency of such mechanisms, also leaving one major actor unheard in the process.

114 Article 16 of the E-commerce Directive 2000/31
115 Article 17 of the Directive 2004/48 on enforcement of IPR
116 Article 13 (3) of the Proposal for a Copyright Directive
Mechanisms resolving copyright infringements (removal of the content, termination of the account) found in these codes impinge on the fundamental right of privacy, freedom of expression and information. In accordance with ECHR these rights are not absolute, they can be restricted only by judicial authorities following a fair trial.\footnote{P.B.Hugenholtz, “Codes of conduct and copyright enforcement in cyberspace” in Stamatoudi I. (ed.), “Copyright Enforcement and the Internet”, Wolters Kluwer International, (2010), pp. 303-320} Simple removal by ISPs without hearing the other side can be considered contrary to ECHR.

As codes of conduct represent agreements of preferable behaviour among ISPs, one of the drawbacks is that their enforcement shall be as of any other contract.\footnote{Ibid, pp. 306-308} If peer pressure of other ISPs does not influence the one refusing to follow the code of conduct, long and expensive civil proceedings may be the only solution.

The Dutch NTD Code of Conduct is an example of the co-regulation between the government and stakeholders. It went beyond Dutch law in order to clarify the responsibilities of ISPs when they encounter unlawful content. The Code of Conduct recognises three types of content: punishable content usually contrary to criminal law, unlawful content contrary to civil law and ‘undesirable’ content which is not contrary to the Dutch law, but the provider does not want to host it. Here the focus will be on the two latter categories.

For the content to be removed, the Code lays down the order of steps to be taken. The notifier\footnote{Article 2(b) of the Notice and Take Down Code of conduct “The notifier is a person or organization that makes a report” regarding the copyright infringing content; in “Notice and take down code of conduct”, Version 1, (2008) available at https://www.ecp.nl/sites/default/files/NTD_Gedragscode_Engels.pdf , last accessed on 30.01.2018.} should first request the removal from the content provider\footnote{Article 2(c), ibid “The content provider is the person (or organization) that has placed (contested) content on the Internet”;}. As content providers are not always known, the notifier then turns to the most appropriate intermediary\footnote{The most appropriate intermediary will be determined from the circumstances of the case, it could be owner of the website, or the host of the website or the access provider. Further reference: “Notice and Take Down code of conduct”, Version 1, (2008) available at https://www.ecp.nl/sites/default/files/NTD_Gedragscode_Engels.pdf pp. 6, last accessed on 30.01.2018.} by submitting a report providing necessary information, and upon which an ISP has a couple of choices. “Where there is no doubt concerning the unlawfulness under the civil law of the content concerned, the intermediary should immediately take measures...
that lead to the content being taken off-line.”\textsuperscript{122} However, there are cases when ISPs cannot “unequivocally determine whether the content is unlawful”\textsuperscript{123}. When this happens, ISPs should first request the content provider to remove the questionable content willingly. If they do not comply, ISPs can decide to take down the content, or to provide the notifier with the content provider’s contact.\textsuperscript{124} Under Dutch law, ISPs do not have an obligation to retain their clients’ data nor can they be forced to reveal personal data.\textsuperscript{125}

The category of unwanted content is particularly confusing as it allows the removal of content that is not unlawful but simply unwanted. However, the Code does not provide any guidelines to what can be considered ‘unwanted’, which means that ISPs can become private censors.

Although providing some clarity to ISPs, the Code has left some questions unanswered. It decided not to “even mention the right to freedom of expression and the issue of censorship”\textsuperscript{126}. Judiciary role imposed on ISPs in instances when the content cannot be proclaimed unequivocally unlawful, may have a strong effect on fundamental rights.

Generally speaking, ISPs prefer self-regulation over statutory, as they have more influence on its formulation. This could also be said for some major right holders as they are more actively involved when compared to statutory procedure. However, the Code of Conduct functions the best if fundamental rights and principles are regulated by law and the Code is used as an annex to the law. It should focus on issues which are usually not regulated by law such as technical issues, a detailed procedure, education of users, etc. Additionally, representation of users is necessary as they are also the key stakeholder, otherwise the democratic nature is seriously endangered.

\textsuperscript{122} “Note to article 6b”, ibid
\textsuperscript{123} “Note to article 6c”, ibid.
\textsuperscript{124} Article 6c of the NTD Code of Conduct
\textsuperscript{125} Case law has provided some criteria on when ISPs should provide the notifiers with the content provider’s information: when the content: “could be unlawful in respect of the notifier, lead to damage being caused to the notifier, or if a less drastic way to obtain the name and contact details is unavailable to the notifier”. Further reference: “Note to article 6c”, ibid.
6.3 Mechanism established by a private entity – Content ID

Mechanisms established by private parties are usually used as an additional measure to ensure that they act in a legal manner enabling them to enjoy immunity from liability for third party content.

Such mechanisms usually have the form of content recognition technologies, which are able to recognise targeted content and perform certain acts (disable access to it in whole or in part, mute it, etc.). Usually, host providers who are hosting excessive quantities of third party content use CRT in order to ensure prompt recognition and removal of the infringing content. Positive aspect of a mechanisms established and enforced by a private party is that they are tailor-made for the needs of specific ISP, and therefore function better than generally imposed mechanisms. However, as the design of such mechanism is solely in the hands of a private party without the involvement of authorities, unlike with previous mechanisms, ‘democratic deficit’ is evident. Additionally, this is expensive technology which can be challenging for less affluent platforms, hence CRT might not be ‘a one-size fits all’ solution.

There are many content recognition technologies in use, yet the Content ID is widely known as it is implemented by YouTube. Content ID is necessary on platforms such as YouTube because the quantity of content uploaded, (300 hours per minute), makes it impossible for manual examination.

Content ID can be considered as a contractual and technical tool used by YouTube “increasing a copyright holder’s control over every use of their work”.

It consists of a database and an algorithm. The database is composed of ‘reference files’, audio and video recordings submitted by the “right holders which have exclusive

---

128 Example: ACRCloud, Audible Magic, Digimarc, Gracenote, Kantar Media, Shazam, etc.
rights to the submitted material”\footnote{Further reference: “Qualifying for Content ID” available at \url{https://support.google.com/youtube/answer/1311402?hl=en&ref_topic=2778544}, last accessed on 30.01.2018.} while the algorithm compares every file uploaded to the database and applies certain policies.

Content ID scans uploaded files, in its search for registered files and, upon finding them, conducts a policy chosen by the right holder. It will either “block it, mute it, make it unavailable on certain platforms, monetize it or track it”\footnote{For further reference see: "Copyright strike basics" available at \url{https://support.google.com/youtube/answer/2797370?hl=en}, last accessed on 30.01.2018.}. If Content ID spots ‘reference files’ uploader gets a Content ID claim which they can dispute, in which case YouTube will notify the right holder leaving him 30 days to respond.\footnote{For further reference see: “Dispute a Content ID claim”, available at \url{https://support.google.com/youtube/answer/2797454}, last accessed on 30.01.2018.}

Right holder can choose to withdraw the claim (or not respond to the dispute), uphold it or request for the infringing file to be taken down. If the file is taken down, the uploader will get a copyright strike. The copyright strike will last for 90 days if user completes an educational course. If a user accumulates three strikes the “account will be terminated, videos removed and the user will not be able to create new channels”\footnote{See “Copyright strike basics” available at \url{https://support.google.com/youtube/answer/2814000}, last accessed on 30.01.2018.}. On the other hand, right holder can file an unlimited number of claims, regardless if they are legitimate or groundless. However, if right holder repeatedly makes groundless or unjustified claims, YouTube can terminate partnership with him.\footnote{DeLisa, Nicholas Thomas. "You(Tube), Me, and Content ID: Paving the Way for Compulsory Synchronization Licensing on User-Generated Content Platforms.” \textit{Brooklyn Law Review} 81.3 (2016), 1275-1317.} This is highly unlikely to happen if the right holder is someone like UMG, WMG or Sony, which demonstrates unbalanced legal positions of right holders and users.

User can also submit a counter notification if his “upload was removed or disabled as a result of a mistake or misidentification of the material, for example, fair use”\footnote{Further reference “Counter Notification Basics” available at \url{https://support.google.com/youtube/answer/2807684}, last accessed on 30.01.2018.}. Upon the processing of the counter notification, YouTube will forward it to the right holder who has
to provide the proof that he/she has initiated a court action in order to keep the content down.

As Content ID, CRTs have positively affected both right holders and users. Monetisation of uploaded contents satisfies the public as they have access to the work, but also the right holders as it gives them revenue. Additionally, right holders can choose to track the content which was recognised by Content ID, allowing it to stay available and economically benefit the copyrighted work. The same content would otherwise be removed according to legal provisions, implying that CRT, in a sense, distorts legal provisions. As for the ISPs hosting excessive amount of content, automatization is the only answer to fight infringement.

However, there are also downsides to CRTs. Available CRTs are not delicate enough to determine if a use is licensed, if it is within the limits of ‘fair use’ or some form of derivative work. Consequently, it discourages creators to apply for a license and applies ‘fair use’ in reverse: it is not ‘fair use’ until proven contrary. As an example, Content ID even reported videos from Warner Bros. Picture official channel as infringing to Warner Bros. Picture rights. Due to the automatization, videos containing criticism and reviews are taken down if they use parts of copyright-protected work, as the algorithm does not distinguish it from egregious infringements. This could be solved by allowing CRT to shut down what is unambiguously illegal content, while in the event of criticism or review ask for human assistance for detailed examination.

In the case of Content ID application per se is restrictive, since the submission of reference files is available only for right holders who have a “substantial amount of content

---

136 This is usually done to attract publicity to copyright protected work.
138 Other cases of Content ID mistakes, Julia Reda, “When filters fail: These cases show we can’t trust algorithms to clean up the internet” available at https://juliareda.eu/2017/09/when-filters-fail/, last accessed on 30.01.2018.
139 Any form of violence, abuse, etc.
on YouTube”. Consequently, a creator must have a record or a publishing deal or sign a contract with MCN.

Disadvantage pointed out by founders of major platforms and applications such as SoundCloud, Musical.ly, Twitch.tv, Dubsmash, and Vine is that they would have never existed if technologies as Content ID had been obligatory at the time of their founding. Consequently this could mean that CRT can be an obstacle for further creative, technological and economic development for both new and existing companies.

Additionally, it is not too complicated to circumvent Content ID by using a reverse image, altering pitch and the speed of the song, including muted parts of a song, etc.

As a conclusion, CRTs as Content ID, are a necessity for hosts with large amount of third party content, though complete automatization has some disadvantages. In order to minimise the disadvantages ISPs should consider adding a human character to the process as the technology applicable is not sensitive enough to detect subtle differences hence restricting the right to expression and information. In addition, any CRT used should be available to all right holders and not only to those with the ‘substantial amount of content’. Lastly, mechanisms such as Content ID are established by a private entity, therefore their transparency should be imperative in order for users and right holders to know what to expect and how to protect their rights and interests.

---

140 DeLisa, Nicholas Thomas. "You(Tube), Me, and Content ID: Paving the Way for Compulsory Synchronization Licensing on User-Generated Content Platforms. Brooklyn Law Review 81.3, pp. 1275-1317

141 Multichannel networks – aggregate content and cooperate with YouTube just as a record company. However, to sign with MCN you have to have a certain number of subscribers. For further reference: DeLisa, Nicholas Thomas. "You(Tube), Me, and Content ID: Paving the Way for Compulsory Synchronization Licensing on User-Generated Content Platforms." Brooklyn Law Review 81.3, (2016), pp.1275-1317

On the path to the creation of Digital Single Market, the EU will have to resolve the issue of cyberpiracy and regulate the status of ISPs in order to secure proper, and uninterrupted functioning of information services.

Compared with other topics, ISP’s liability and digital piracy are more challenging for a legal system as they continually develop at a high speed. Therefore, this may be one of the areas in which EU should not aim for unification or harmonization but flexibility.

After reviewing the existing EU legal framework and CJEU decisions it is certain that any solution to digital copyright infringements ought to be sought within existing principles and boundaries. The EU has already taken some steps through Article 13 of Proposal for Copyright Directive, which confirmed that future solutions ought to be compatible with the established exemptions from ISPs’ liability and prohibition of mass surveillance. A solution contrary to this would disrupt the existing system, causing confusion and misinterpretation rather than enhancing legal certainty for fundamental rights.

In author’s opinion, the EU should seek to reach an agreement regarding principles, objectives and goals it aspires to achieve in the battle against cyber piracy and collect them in a form of regulation, securing their direct implementation in each Member States.

Furthermore, until this moment EU has accumulated enough experience through the CJEU case law and national mechanisms as French ‘three strike system’. These experiences should be formulated in a set of new directives focusing on regulation and enforcement of IPRs specifically in cyberspace with obligatory revision.

In addition to legislative actions, the EU should put greater focus on prevention of infringements. Education of general public has shown positive results in preventing infringements thus decreasing the need for judicial proceedings and repressive measures. Additionally, the development of a sophisticated CRT which would take down evidently infringing content aided with human assistance in more complex situations, would create an environment where only the most persistent and ignorant infringers would be prosecuted.
As ISPs are the main actors ensuring the flow of information services, their neutral status is undoubtedly essential for proper, and uninterrupted functioning of the Internet. Therefore, ISPs must retain neutral status as long as they follow conditions established by the E-Commerce Directive. On the other side, if an ISP uses its immunity to perform or contribute to infringing activities, its liability must be certain. However, in order to protect other fundamental rights, they should not act as private censors or judges. The decision regarding the balance of fundamental rights and their restriction must remain within the hands of EU authorities.

Copyright holders will have to modify their approach to digital environment if they wish to properly exercise their rights. It is highly unlikely for them to expect that digital environment will be adapted through legislation in order to facilitate their needs. Film and music industries among others will have to modify and adjust their businesses to cyber environment, rather than hold onto traditional, offline business models.

The same can be said for fundamental rights to privacy and freedom of information. Their safeguarding will have to take full advantage of new technologies and the end users will have to become aware that cyberspace will not provide an escape from liability.

As a conclusion, time will be necessary for the adjustment of public behaviour and actions of authorities to combat cyber piracy. During that period, the EU must remain the leader and must not transfer challenging decisions to ISPs. This effort is certainly worth as the Internet opens up a whole new world of possibilities and opportunities.
8. Bibliography

Books


Articles


22. Reda, Julia “When filters fail: These cases show we can’t trust algorithms to clean up the internet” available at https://juliareda.eu/2017/09/when-filters-fail/ , last accessed on 30.01.2018.


24. Rosati, Eleonora, “CJEU says that blocking orders are OK and do not have to be specific” available at http://ipkitten.blogspot.rs/2014/03/breaking-news-cjeu-says-that-blocking.html, last accessed on 30.01.2018.


Philosophical Enquiry” from 8th International Conference Corfu 26-28 June 2009
Ionio University, Nomiki Vivliothiki, Athens, Greece, (2009), pp. 757-767.

Telefonica & Lsg v. Tele2”, Revue Hellenique de Droit International vol. 63, no. 2,
(2010), pp. 921-948.

32. Stamatoudi, Irini, “Data protection, secrecy of Communication and Copyright” in
Stamatoudi I. (ed.) “Copyright Enforcement and the Internet”, Kluwer International

and problems” in “4th International Seminar on Information Law”, University of
Thessaloniki (Aristoteleio), University of Macedonia and Ionio University,

34. Strowel, Alain, “The Graduated Response in France: Is it good to reply to online
copyright infringements?” in Stamatoudi Irini (ed.), “Copyright Enforcement and the
Internet”, Kluwer Law International BV, the Netherlands, (2010), pp.147-162.

Online sources

1. “Counter Notification Basics” available at
https://support.google.com/youtube/answer/2807684, last accessed on
30.01.2018.

2. “Deconstructing the Article 13 of the Copyright proposal of the European
Commission” available at
https://edri.org/files/copyright/copyright_proposal_article13.pdf, last accessed on
30.01.2018.

3. “Digital single market - Bringing down barriers to unlock online opportunities”
available at https://ec.europa.eu/commission/priorities/digital-single-market_en,
last accessed on 30.01.2018.
4. “GDPR Key Changes: An overview of the main changes under GPDR and how they differ from the previous directive” available at [https://www.eugdpr.org/key-changes.html](https://www.eugdpr.org/key-changes.html), last accessed on 30.01.2018.


EU legal framework

1. Charter of the fundamental right of the EU.
7. Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

National legislation

2. The Dutch Notice and take down code of conduct.
CJEU Case law

1. Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV (C 360/10).
2. L’Oréal SA and others v eBay International AG and Others (324/09).
3. LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH (C-557/07).
4. Opinion of Advocate General Kokott regarding case Promusicae v Telefonica (C-275/06).
5. Patrick Breyer v Bundesrepublik Deutschland (C-582/14).
6. Productore de musica de Esana (Promusicae) v Telefonica de Espana (C 275/06).
7. Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (C-70/10).
8. UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH (Case C-314/12).