ISSN 2003-2382

The effectiveness of blocking injunctions against ISPs in respect of online copyright infringement in Europe: a comparative analysis from the UK, Greece and the Nordic countries

By Despoina Farmaki

ABSTRACT

Blocking injunctions against Internet Service Providers (ISP) are a common and valuable remedy in cases of online copyright infringement. This paper focuses on the effectiveness of blocking injunctions against ISPs in Europe. An understanding of the key legal concepts and procedures is provided. Emphasis is given to the interpretation of the "act of communication to the public". Doctrinal and comparative research methods have been deployed to examine how the selected jurisdictions respond to blocking injunctions. The paper provides recommendations to increase the effectiveness of blocking injunctions through EU harmonisation, while it also provides alternative measures to tackle online copyright infringement.

1. INTRODUCTION

> *"The internet is the largest and most efficient copying machine built by man".*[1]

Murray sees the development of the internet and the shift from the physical to digital distribution models as two of the "most disruptive events of the twentieth century".[2] Although the internet promotes communication, electronic commerce, freedom of expression, and the right to information, its diversified content could be illegal at many levels, from criminal activities and fraudulent actions to infringement of intellectual property rights. Despite the benefits that the internet provides to the right holders in terms of a mass audience, allowing authors to distribute their work freely to consumers, it also entails the danger of online intellectual property infringement by uncontrolled copying and piracy.

In the case of online copyright infringement, it is time-consuming and burdensome for the right holder to reach the offender, as well as it is costly to start proceedings for the enforcement of their rights. Thus, it would be more sensible for right holders to shift their attention from individuals to intermediaries. However, in most cases, the intermediary's liability is not a direct one; the intermediary is not usually the party who directly and with intention committed the infringement, but rather provided the service by which the infringement was committed. In the online world, it is of the utmost importance to take measures not only to detect current infringement, but also to prevent further infringements.

For many years, copyright owners had at their disposal the Notice and Takedown tool to notify internet intermediaries and ask for the removal of the infringing content. However, there is a real possibility that through the removal, even legitimate content may be removed. Thus, an independent, unbiased and balanced mechanism should be deployed.[3]

For that reason, a new approach gained popularity in the European Union (hereinafter the EU), by which right holders could apply to the courts, seeking an injunction that will compel ISPs to block access to infringing websites.

The aim of the paper is to mainly focus on blocking injunctions which have been granted against ISPs in respect of online copyright infringement in Europe. Through the employment of doctrinal and comparative methods, the paper aims to explore how the different jurisdictions have responded to the "act of communication to the public" and in consequence to the blocking injunctions. At the same time, it will examine whether blocking injunctions alone could effectively tackle online copyright infringement.

Doctrinal research is the process used to identify, analyse and synthesise the content of the law.[4] In general, primary sources, including relevant and available conventions, EU legislation, statutes, and case law will be assessed. In addition, analysis of the domestic laws of the selected jurisdictions is undertaken to provide a comprehensive assessment of the effectiveness of blocking injunctions in the EU. The analysis will focus on the approaches of the UK, Greece, and the Nordic countries, as these jurisdictions demonstrate a typical example of jurisdictions whose national courts grant blocking injunctions for copyright infringement.

The following section will define the key legal concepts and procedures. It will start with an understanding of the blocking injunctions and will introduce the website blocking techniques. After explaining the importance of copyright as an intellectual property right, it will introduce the ISP and will move to their responsibility and liability. The paper will proceed with the determination of the "communication to the public", as one of the exclusive rights of copyright holders. Exploring the "act of commu-

nication to the public" is very crucial, since blocking injunctions have been granted due to infringement committed through this restricted act. While the paper aims at presenting how the selected jurisdictions respond to blocking injunctions, by examining the domestic laws and cases from the UK, Greece, and the Nordic countries, it will raise some concerns regarding the potential of collateral damage and the reality of circumventing blocking orders. Based on the relevant legislation and case law, recommendations will be provided on how blocking injunctions could be more effective, through EU harmonisation. Meanwhile, it will provide alternative measures on how to tackle online copyright infringement in a more effective way.

2. UNDERSTANDING THE BLOCKING INJUNCTIONS AND THE ISPS

2.1 Understanding the blocking injunctions: the legal framework

The blocking injunction is one of the most popular remedies among intellectual property right holders to enforce their rights in the digital environment. The aim of obtaining a blocking injunction is to compel an ISP to block access to websites that contain infringing content.[5]

The European legislative basis for a website-blocking injunction is Recital 59 of Directive 2001/29 on the harmonisation of certain aspects of copyright and related rights in the information society (hereafter the Information Society Directive) which states that third parties may use the services of intermediaries for infringing activities.[6] It continues 'therefore...right holders should have the possibility of applying for an injunction against an intermediary'. In addition, Article 8(3) of the Information Society Directive requires Member States to ensure that intellectual property right holders can 'apply for injunctions against intermediaries whose services are used by a third party to infringe a copyright or related right'.[7]

In a similar way, Recital 23 of the Directive 2004/48 on the enforcement of intellectual property rights (hereafter the Enforcement Directive) states that right holders can apply for injunctions against an intermediary whose services are used by a third party in order to infringe the right holder's industrial property right.[8] Additionally, Article 3 of the Enforcement Directive provides that 'Member States should provide for the measures, procedures and remedies...to ensure the enforcement of the intellectual property rights'[9] as well as Article 11 of the Enforcement Directive provides that 'Member States shall ensure that the judicial authorities may issue against the infringer an injunction' with the aim to prohibit the continuation of the infringement.[10]

Following Article 8(3) of the Information Society Directive, the Court of Justice of the European Union (hereinafter the CJEU) confirmed in the landmark case of *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH*[11] that the granting of blocking injunctions against ISPs harmonises with the EU law. The court specified that blocking injunctions can be granted in national courts where it is balanced as well as proportionate, having regard to the right holder's intellectual property rights, the ISP's right to conduct a business, and the user's right to access information.[12] According to the judgement, ISPs have to consider the fundamental right of the internet users to freedom of information on the one hand and the adoption of effective measures as to the prevention of unauthorised access to the protected subject-matter on the other hand.[13]

2.2 Website-blocking techniques

There is a variety of blocking techniques that the ISPs can adopt in order to block a target website or an online location. In the UK High Court's *Cartier v. Sky*[14] case, Justice Arnold referred to four blocking techniques, namely the Domain Name System (DNS) blocking, the Internet Protocol (IP) blocking, the Deep Packet Inspection (DPI)-based Uniform Resource Locators (URL) blocking as well as the two-stage systems.

2.2.1 Domain Name System (DNS) blocking

The first blocking technique is known as DNS blocking. To gain a better understanding of the DNS blocking, an explanation should be given to the translation process between the DNS and the Internet Protocol (IP) address. Devices connecting to the internet bear a unique IP address.[15] However, these addresses are hard to remember. In an effort to avoid any difficulties, IP addresses are translated into domain names. For instance, Google's search page has as its IP address the number '64.233.167.99', which corresponds to the domain name 'google.com'.[16] As a result, every time a user requests 'google.com', that request has to be translated into the corresponding IP address for the devices to connect. This process is done using the DNS.

1 A. Murray, *Information Technology Law The Law and Society* (3rd edition, Oxford University Press 2016) 275.
2 Ibid.
3 A. Marsoof, 'The blocking injunction – a critical review of its implementation in the United Kingdom in the context of the European Union' (2015) 46(6) IIC 632.
4 D. Watkins and M. Burton, *Research Methods in Law* (2nd edition, Routledge 2018) 13.
5 A. Roy and A. Marsoof, 'Blocking injunctions and collateral damage' (2017) 39(7) European Intellectual Property Review 74.
6 Council Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L 167/10, Rec. 59.
7 Ibid Article 8(3).
8 Council Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights [2004] OJ L 157/45, Rec. 23.
9 Ibid Article 3.
10 Ibid Article 11.
11 Judgement of 27 March 2014, *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH, VerleihGmbH*, C-314/12, ECLI:EU:C:2014:192.
12 Ibid paras 46-47.
13 Ibid paras 55,56,62.
14 *Cartier International AG &Ors v British Sky Broadcasting Ltd &Ors* [2016], EWCA Civ 658 [25].
15 Roy and Marsoof (n 5) 74.
16 Ibid.

The DNS blocking uses the translation process in order to block access to websites containing infringing material. ISPs remove or modify their records of the IP address for a specific DNS name, so that when a customer's computer asks the ISPs' DNS server for the IP address that corresponds to the DNS name, the ISPs' system can either return no IP address or redirect the customer to another site, informing users that access has been blocked.[17]

2.2.2 The Internet Protocol (IP) blocking

The second blocking technique is known IP blocking. This technique will prevent connections between any particular device and hosts whose IP addresses are blocked. The IP address system operates by means of routers.[18] Thus, an ISP is able to configure its routers to discard any communication destined for the IP address in question or can route them to another IP address defined by them, which in fact is different from the actual IP address of the website.[19] As a result, even if a customer's computer uses the correct IP address for the website in question, this technique blocks any communication to the website.

2.2.3 The Uniform Resource Locator (URL) site blocking

The URL is the address of a specific document or a specific file on the World Wide Web.[20] It includes a domain name and the location of the specific file or document. Compared to the DNS or IP address blocking, this method requires more scrutiny of data packets so as to determine the exact address of the file or document.

This technique is implemented by an ISP rerouting traffic to a proxy server that has a list of blocked URLs. When a customer requests a URL, the next step is the comparison between the requested URL with those in the blacklist. In case the requested URL matches one of the listed URLs, the connection is either refused or redirected to another website.[21]

The URL blocking requires packet inspection and may involve either shallow packet inspection (SPI) or deep packet inspection (DPI). DPI analyses all the content of data packets that pass through the network, the headers, and the data protocol structures, while the SPI focuses on analysing the packet header. The distinction between the functioning of the DPI and the SPI is the capability of the DPI to analyse all layers of data packets sent across the internet. Wanger emphatically compares the DPI technology to an automated system within the postal service that may open each letter, checks the content of the letter and modifies it as necessary, then reseals the letter and sends it on its way.[23]

2.2.4 The Hybrid systems

The hybrid blocking involves the combination of the abovementioned techniques and often implements a two-stage approach. For instance, the IP address blocking could be used as the first stage in order to direct potentially blocked websites to a proxy server which in turn engages in a packet inspection to block access to a specific URL.[24]

This hybrid approach has the potential to be used in order to reduce the impact on the performance of the network and improve the effectiveness of the blocking as it will make circumvention difficult.[25] A hybrid method has been developed by British Telecom, under the name 'Cleanfeed', which deploys a two-stage mechanism: IP address blocking and DPI-based URL blocking in order to filter specific internet traffic.[26]

2.3 The responsibility and liability of ISPs as intermediaries

2.3.1. Defining the ISP

An ISP is any person or entity that provides an information society service for remuneration through electronic means for the processing and storage of data relying on any platform of electronic communication.[27] In order to gain a better understanding of who qualifies as an ISP, emphasis should be given to the meaning of the 'information society service'. An information society service is 'any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing and storage of data, and at the individual request of a recipient of the service'.[28] Some of the information society services may include online sale of goods, web hosting, internet access services, and internet transit.[29]

Where an ISP provides information society services, it is inevitable that the ISP is open to potential liability arising from the misuse of the service by the recipient. The recipient of the service is a natural or legal person who uses the service to seek information or to make such information accessible.[30] Potential liability could arise as a consequence of the content provided through the platform or the storage of materials on the platform.

17 D. Lindsay, 'Website blocking injunctions to prevent copyright infringements: proportionality and effectiveness' (2017) 40(4) UNSW Law Journal 1507.

18 Ibid.

19 Roy and Marsoof (n 5) 74.

20 Lindsay (n 17) 1507.

21 Ibid.

22 B. Wanger, 'Deep packet inspection and internet censorship: International Convergence on an 'Integrated technology of control' (2015) Global Voices Advocacy Defending Free Speech Online (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2621410) accessed 18 October 2021.

23 Ibid.

24 Lindsay (n 17) 1507.

25 Ofcom, 'Site Blocking to Reduce Online Copyright Infringement: A review of Sections 17 and 18 of the Digital Economy Act' (Ofcom, 27 May 2011) (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/78095/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf) accessed 18 October 2021.

26 *Twentieth Century Fox and others v. British Telecommunications plc* [2011] EWHC 1981 (Ch) [73].

27 Council Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [2000] OJ L 178/1, Article 2(b).

28 Ibid Article 4.

2.3.2. ISP and its liability

Before examining ISPs' liability, it is important to discuss their responsibility. It is hard for copyright owners to identify and initiate proceedings against the users and the website operators, who may reside in a non-EU jurisdiction. ISPs, however, can easily identify a particular infringing website, and economically it is more efficient to require intermediaries to take action to prevent infringement occurring via their services.[31]

Intermediaries' liability is embodied in Articles 12-15 of Directive 2000/31 (hereafter the E-commerce directive).[32] After reviewing the content of the legislation, one could argue that the immunity does not apply to the provider of the service, but to the activity.[33] Intermediaries liability and the exemptions to the said liability are available provided that the intermediary acts as a mere conduit, caching, or hosting service provider.

2.3.2.1 Mere Conduit

An ISP acts as a mere conduit where it plays a transient or passive role in aiding the transmission of information on behalf of content providers.[34] For instance, BT as a means of accessing internet services, enables UK users to connect to the internet. When providing access to the internet, an ISP can claim certain exceptions from liability under the conditions that the intermediary is not responsible for initiating the transmission, selecting the person receiving the information, and must not interfere or modify the content of the transmission.[35] In case that the intermediary takes any active steps, the available exemptions will cease to apply.

Although intermediaries enjoy immunity when functioning as 'mere conduits', the Belgian court in the *SABAM v Scarlet*[36] case reached a controversial judgement. SABAM aimed at compelling Scarlet to install filtering software with the view to restrict the transmission and sharing of copyrighted music through the ISPs' network.[37] Although Scarlet argued that it only provides internet access to its customers and no other services, such as file-sharing or download, the court ordered the ISP to install filtering software aiming at identifying and blocking access to copyright-protected music. However, the CJEU stated that it is unreasonable to request ISPs to install filtering software for the purposes of copyright protection.[38]

2.3.2.2 Caching

Caching is the transmission of information at the request of a recipient who stores the information for a short period in order to transmit that information efficiently. Adeyemi argues that this practice equals a better internet speed since the efficient use of server spaces and internet cables makes space available for other users.[39]

The immunity of intermediaries is based on the fact that they do not interfere with the information passing through the network by modifying it and that they update the information regarding terms of use on a regular basis.[40] Nevertheless, the storage of information for a longer period of time would amount to stricter requirements for exemption from liability. Article 13 on caching aims to protect intermediaries in respect of materials that do not originate from them but are temporarily stored on their servers.[41]

2.3.2.3 Hosting liability

Article 14 refers to the liability of intermediaries that provide hosting services. In this situation, intermediaries store information provided by the recipient of the service. The storage of information refers to holding, keeping, or storing information on a server.[42] The host provides the server for storing the website so as to be accessed by users. In other words, the recipient generates the content and places it on a server so that it is easily accessible by users.

[29] A. Adeyemi, 'Liability and exemptions of internet service providers (ISPS): assessing the EU electronic commerce legal regime' (2018) 24(1) Computer and Telecommunications Law Review 6.

[30] Council Directive 2000/31/EC (n 27) Article 2(d).

[31] *Cartier International AG &Ors v British Sky Broadcasting* EWHC 3354 (Ch); [2015] 1 All E.R. 949.

[32] Council Directive 2000/31/EC (n 27).

[33] EU Commission, 'First Report on the Application of Directive 2000/31/EC' (Brussels 21.11.2003, COM(2003) 702 final) section 4.6 (http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2003/0702/COM_COM(2003)0702_EN.pdf) accessed 18 October 2021.

[34] Council Directive 2000/31/EC (n 27) Article 12.

[35] Ibid.

[36] *SABAM v SA Tiscali (Scarlet)*, District Court of Brussels, No. 04/8975/A, Decision of 29 June 2007.

[37] Ibid.

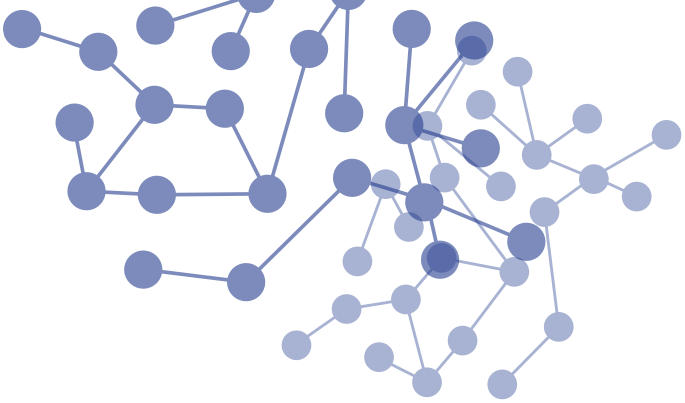
[38] Judgment of 24 November 2011, *Scarlet Extended SA v SociétéBelge Des Auteurs, Compositeurs Et Éditeurs SCRL (SABAM)*, Case C-70/10, ECLI:EU:C:2011:771.

[39] Adeyemi (n 29) 6.

[40] Ibid.

[41] Council Directive 2000/31/EC (n 27) Article 13.

[42] Adeyemi (n 29) 6.



Article 14 is applicable to a wide range of providers such as online marketplaces, blog services, social media platforms, and operators of interactive sites. For an ISP to claim an exemption under Article 14 of the E-Commerce Directive, the following conditions need to be fulfilled:

1. the service in question must qualify as an information society service,
2. the service consists of the storage of information,
3. it is provided by the recipient of the information,
4. the provider does not have actual knowledge (or is not aware of the illegal nature of the information), or upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.[43]

The content hosted on the servers is not pre-approved by the hosts.[44] They are afforded a reasonable opportunity to remove the infringing material or illegal content after receiving notice to do so.

3. DETERMINATION OF THE "COMMUNICATION TO THE PUBLIC"

One of the exclusive rights of copyright holders that has been outlined in Article 3 of the Information Society Directive is the right of "communication to the public of works and right of making available to the public other subject-matter".[45] The Berne Convention[46] also recognises the rights of "public performance", "communication to the public" and "public recitation". The World Intellectual Property Organisation (hereinafter the WIPO) Copyright Treaty in its Article 6 and 8 provides for the right of making a "work available to the public".[47] The WIPO Performances and Phonograms Treaty provides for a right of making available their subject matter to the public and Article 15 refers to "a right of communicating the relevant work to the public".[48]

In the digital context the problem of unauthorised "act of communication to the public" arises in cases where third parties subsequently retransmit content that had been initially communicated by the right holders.[49] For example, protected work that was available on a website may be accessible from another website or via an email including a hyperlink.

Although the CJEU held in the *Sociedad General de Autores y Editores de Espana v. Rafael Hoteles*[50] that the EU should give an "autonomous and uniform interpretation" to the notion of "communication to the public" subsequent CJEU judgements have begun to bring some clarity to the determination of the "communication to the public".

3.1. An act of communication

As far as the first element of "an act of communication" is concerned, it depends on whether the user has played an "indispensable role" through a "deliberate intervention".[51] The CJEU applied this principle to the facts of the *Ziggo* case[52] and undoubtedly concluded that the works were made available to the public by the means of The Pirate Bay website. The court established that an "act of communication" entails "any transmission or retransmission of a work to the public by wire or wireless means, including broadcasting".[53]

It further continued with the confirmation that "any act by which a user, with full knowledge of the relevant facts, provides its clients with access to protected works is liable to constitute an 'act of communication' for the purposes of Article 3(1) of Directive 2001/29".[54] The next step was to determine who was responsible for this act. The court acknowledged that it was the users who placed the work on the platform, not The Pirate Bay itself.

However, the court concluded that the management of an online sharing platform amounts to a deliberate intervention. In an effort to support this argument, the court observed that in absence of The Pirate Bay, it would be either impossible or more difficult for users to share materials online. In addition, the platform indexed the torrent files in a way that made it easy to locate and download them, and classified the works under different categories.[55] Last but not least, the platform's operators had an active role such as checking the categories, deleting faulty torrent files and filtering some content.[56] The acts of indexing the torrent files so that they would be easy to locate and download, the categorisation of different works, and the active role that the operator played, undoubtedly constitute intentional interference and thus copyright infringement.

3.2 The public

As far as the second element of "the public" is concerned, the judgement on the *Ziggo* case is compatible with the previous judgement on *Strichting Brein v Jack Frederik Wullems*.[57] The CJEU defined the public as a group of people of an indeterminate number that is of a certain, not insignificant size;[58] using specific technical means, different from those previously used;[59] or the work was communicated to a "new public" that was not taken into account by the copyright holders when they authorised the initial communication of their work to the public.[60] In *Sociedad General de Auditores y Editores (SGAE) v. Rafael Hoteles SL* and *Organismos Sillogikis Diacheirisis Dimiourgon Theatrikon kai Optikoakoustikon Ergon v. Divani Acropolis Hotel,*[61] the court held that "a transmission made to a public different from the public at which the original act of communication of the work is directed, that is to a new public". Thus, the clientele of a hotel, for example, forms a new public.

It is also worth mentioning that there is not a requirement of reaching the audience simultaneously. As Angelopoulos stated, the cumulative effect of making works available to the public in succession has to be taken into consideration.[62] Examining the facts of the case, it was

easy for the court to rule that the considerable number of users who used The Pirate Bay met the second criterion, since The Pirate Bay was targeted at an indeterminate number of potential recipients.[63] Regarding the concept of the "new public" the court held that "such a public is a public that was not taken into account by the copyright holders when they authorised the initial communication".[64]

When the copyright owner creates a work, he/she wishes for that work to reach as many recipients as possible. However, it is a completely different situation when the work "escapes" from the copyright owner's attention and reaches a different, wider and new public that was not taken into account at the time of the first communication. The fact that online services provide access to copyright-protected content without the involvement of right holders, has affected right holders' possibilities to determine whether and under which circumstances their works are used and accordingly their possibilities to get an appropriate remuneration, which has created a 'value gap'.[65] At an EU level, the Digital Single Market Directive[66] has been enacted to 'close this exact value gap.

4. HOW DO THE SELECTED JURISDICTIONS RESPOND TO THE BLOCKING INJUNCTIONS?

Blocking injunctions target ISPs in order to deal with online copyright infringement. However, in absence of harmonised standards, national courts implemented the Information Society Directive in a different way based on their national laws. As a result, courts in some Member States grant blocking injunctions with specific technological orders, while courts in other Member States issue an injunction with non-specific technical measures or do not order ISPs to block infringing websites. The focus of this part will be on the response of the UK, Greece and the Nordic countries (Denmark, Finland, Iceland, Norway and Sweden).

4.1 Blocking injunction in the UK

According to the Motion Picture Association's paper, the UK holds a strong position on the list of European countries that allow the use of website blocking injunctions in cases of online copyright infringement. More specifically, until the year 2018 there were 171 sites blocked in the UK.[67] The legal basis for obtaining a blocking injunction in cases of online copyright infringement is s. 97A of the CDPA 1988.[68]

In the UK there are a number of instances where copyright owners have sought blocking injunctions. The first blocking injunction was granted under s.97A of the CDPA in *Twentieth Century Fox v. BT*.[69] This case was a sequel to a previous dispute between Twentieth Century Fox and Newzbin Ltd, where the latter operated a website under the URL <http://www.newzbin.com> resulting in large scale copyright infringement.[70] Although the High Court issued an injunction against Newzbin to cease operations, a third –unknown- party restored the website from an offshore location. It was impossible for the film production company to seek redress via the court process against that third party. Following a different strategy, Twentieth Century Fox filed an action against BT, an ISP operating in the UK, and sought an injunction compelling BT to block access to the website in question. Justice Arnold who delivered the judgement of the High Court issued a blocking injunction and thus mitigated the impact of copyright infringement within the UK.

[43] Council Directive 2000/31/EC (n 27) Article 14.
[44] Adeyemi (n 29) 6.
[45] Council Directive 2001/29/EC (n 6) Article 3.
[46] Berne Convention for the Protection of Literary and Artistic Works 1886, Articles 11, 11bis, 11ter and 14.
[47] World Intellectual Property Organisation (WIPO) Copyright Treaty1996, Articles 6 and 8.
[48] World Intellectual Property Organisation (WIPO) Performances and Phonograms Treaty 1996, Articles 10,14,15.
[49] S. Karapapa, 'The requirement for a "new public" in EU copyright law' (2017) 42(1) European Law Review 63.
[50] Judgment of 7 December 2006, *Sociedad General de Autores y Editores de España (SGAE) v Rafael Hoteles SA*, C-306/05, ECLI:EU:C:2006:764, para 31.
[51] C. Angelopoulos, 'Communication to the public and accessory copyright infringement' (2017) The Cambridge Law Journal 497.
[52] Judgment of 14 June 2017, *Stichting Brein v Ziggo BV and XS4ALL Internet BV*, C-610/15, ECLI:EU:C:2017:456, para 2.
[53] Ibid para 30.
[54] Ibid para 34.
[55] Ibid para 38.
[56] Ibid para 38.
[57] Judgment of 26 April 2017, *Stichting Brein v Jack Frederik Wullems*, C-527/15, ECLI:EU:C:2017:300.
[58] Judgment of 14 June 2017, *Ziggo* (n 52) para 27; Judgment of 26 April 2017, *Stichting Brein* (n 57) para. 32.
[59] Judgment of 14 June 2017, *Ziggo* (n 52) para. 28; Judgment of 26 April 2017, *Stichting Brein* (n 57) para. 33.
[60] Ibid.
[61] Judgment of 7 December 2006, (SGAE) (n 50) para 40,42; Judgment of 18 March 2010, *Organismos Sillogikis Diacheirisis Dimiourgon Theatrikon kai Optikoakoustikon Ergon v. Divani Acropolis Hotel*, C-136/09, ECLI:EU:C:2010:151, para 38.
[62] Angelopoulos (n 51) 496.
[63] Judgment of 14 June 2017, *Ziggo* (n 52) para. 42.
[64] Ibid para. 44.
[65] European Commission, Communication 'Online Platforms and the Digital Single Market. Opportunities and Challenges for Europe', COM(2016) 288 Final, 8. The 'value gap' refers to the market distortion created by safe harbour provisions for user generated content platforms, leading these platforms to pay less than the market rate for copyright permissions. M. Lambrecht, 'Free Speech by Design: Algorithmic Protection of Exceptions and Limitations in the Copyright DSM Directive' (2020) 11 J. Intell. Prop. Info. Tech. & Elec. Com. L. 68, 70.
[66] Council Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, PE/51/2019/REV/1 [2019] OJ L 130/92, Article 17(1).
[67] Motion Picture Association, Intervention March 2018https://torrentfreak.com/images/mpa-can.pdf 7, accessed 18 October 2021.
[68] Copyright Designs and Patents Act 1988, s. 97A.
[69] *Twentieth Century Fox and others v British Telecom Plc* [2011] EWHC 1981 (Ch).
[70] *Twentieth Century Fox and others v Newzbin Ltd* [2010] EWHC 608 (Ch).

Blocking injunctions were also issued in many cases such as *Dramatico v. Sky*[71], *EMI Records v. Sky*[72], *Football Association v. Sky*[73], and *Paramount Entertainment v. Sky*.[74] In all these cases, injunctions were issued in order to prevent copyright infringement. It is also worth mentioning that in all these cases it was Justice Arnold who delivered the judgement and ordered the blocking injunctions.

Justice Arnold identified four stages of the evolution of the High Court of England and Wales's approach to website blocking.[75] Starting with the *Twentieth Century Fox v. BT and Twentieth Century Fox Film Corp v. British Telecommunications Plc* (No.2) Arnold J stated that in these cases the basic principles and jurisdictional matters were established and the cost apportionment was determined.[76] Later, in *Dramatico Entertainment Ltd v. British Sky Broadcasting Ltd (No.2),*[77] the order was extended to IP address blocking, in the event that the IP address is not shared. In *Football Association Premier League Ltd v. British Sky Broadcasting Ltd,*[78] the website operators have been granted the permission to apply to vary or discharge the order. Finally, according to *Cartier v. BskyB,*[79] the affected users can also apply to vary or discharge the order, the blocked website has to provide for more information to users attempting to access it as well as there was the provision of a two-year sunset clause.

Although the website blocking injunction is a well-known mechanism,[80] a new type of blocking injunctions (live blocking injunctions) appeared in the *FAPL v BT*[81] case. More specifically, instead of seeking to block a whole website, the court order was aimed at immediate, responsive blocking of live streaming transmissions delivering content that infringed the Premier League's copyright.[82] In this case, the live blocking order was possible due to the following technological advances: FAPL used video monitoring technologies that permitted the identification of infringing streams and the ISPs' blocking systems allowed them to block and unblock IP addresses during the course of the Premier League matches.[83] Thus, the UK is a pioneer in live blocking injunctions.

4.2 Blocking injunction in Greece

Article 8(3) of the Information Society Directive has been implemented into the national law in Article 64A of the Greek Copyright Act 1993.[84] Article 64A provides that the right holders are able to grant injunctions against intermediaries, whose services are used by a third party to infringe copyright or related rights. Although Article 64A is of great importance, it did not manage to "produce" sufficient case law. More specifically, this paper will focus on two cases decided by the Greek courts.

In the first case, the collective management organisations "GRAMMO", "ATHINA", "AEPI" and "EPOE" sought to obtain a blocking injunction that would prevent users from accessing the infringing websites <ellinadiko.com> and <music-bazaar.com>.[85] The court ordered the blocking of the websites by the technical means of the IP address blocking. In the second case, the same collective management organisations sought to grant an injunction against the ISPs that would prevent consumers from accessing the same infringing websites. The only difference between those two cases is the fact that, while in the first case the protected materials were available online for downloading, in the second one the websites provided links to other websites. In the second case, the court dismissed the application for a blocking injunction and justified its judgement on the grounds of fundamental free-

[71] *Dramatico Entertainment Ltd v British Sky Broadcasting Ltd* [2012] EWHC 268 (Ch).
[72] *EMI Records Ltd v British Sky Broadcasting Ltd* [2013] EWHC 379 (Ch).
[73] *Football Association Premier League Ltd v British Sky Broadcasting Ltd* [2013] EWHC 2058 (Ch).
[74] *Paramount Home Entertainment International Ltd v British Sky Broadcasting Ltd* [2013] EWHC 3479 (Ch).
[75] R. Arnold, 'Website-Blocking Injunctions: The Question of Legislative Basis' (2015) 37 European Intellectual Property Review 623.
[76] *Twentieth Century Fox Film Corp v British Telecommunications Plc* (No.2) [2011] EWHC 2714 (Ch).
[77] *Dramatico Entertainment Ltd v British Sky Broadcasting Ltd (No.2)* [2012] EWHC 1152(Ch).
[78] Football Association Premier League Ltd v British Sky Broadcasting Ltd [2013] EWHC 2058 (Ch).
[79] *Cartier International AG &Ors v British Sky Broadcasting* [2014] EWHC 3354 (Ch).
[80] K. Garstka and P. Polaski, 'Notice and search-down injunctions in online copyright enforcement: should they be embraced or forgotten?' (2019) 41(3) E.I.P.R. 155.
[81] *The Football Association Premier League Ltd v British Telecommunications Plc & Ors* [2017] EWHC 480 (Ch); [2017] E.C.C. 17.
[82] ibid [24].
[83] *The Football Association Premier League Ltd v British Telecommunications Plc & Ors* [2017] EWHC 480 (Ch) [24].
[84] Greek Copyright Act 2121/1993, Article 64A.
[85] Athens Court of First Instance, Case 4658/2012.
[86] Athens Court of First Instance, Case 13478/2014.
[87] Greek Copyright Act 2121/1993, Article 66E.
[88] Commission for the notification of online copyright and related rights infringement, Decision No. 3/2018, < https://www.opi.gr/images/epitropi/apofaseis/edppi_3_2018.pdf> accessed 11 October 2021.
[89] Greek Copyright Act 2121/1993, Article 66E.
[90] Y. Paramythiotis, 'First blocking orders issued in Greece...but how effective are they' (The IPKat, 9 December 2018) <http://ipkitten.blogspot.com/2018/12/first-blocking-orders-issued-in-greece.html> accessed 18 October 2021.
[91] *Telenor (formerly DMT2 A/S Sonofon A/S) v IFPI Danmark*, Case 153/2009 (27 May 2010, Supreme Court of Denmark).
[92] *IFPI Finland ry v Elisa Oyj*, Case 11/41552 (Helsinki Court of Appeal, 26 May 2011).
[93] J. Songe-Moller and O. K. Foss, 'File sharing, streaming and The Pirate Bay: Nordic perspectives on website blocking' (2016) 22(2) C.T.L.R. 37.
[94] *STEF and SMAIS v Vodafone and Hringdu* (14 October 2014, Reykjavik District Court).
[95] Songe-Moller and Foss (n 93).
[96] *Warner Bros Entertainment Norge AS v Telenor Norge AS*, Case No. 15-067093TVI-OTIR/05 (Oslo District Court, 1 September 2015).
[97] Songe-Moller and Foss (n 93).
[98] Swedish Patent and Market Court of Appeal, *Universal Music AB v B2 Bredband AB* (PMT 11706-15) verdict of 13 February 2017.
[99] N. Malovic, 'Online copyright enforcement in Sweden: the first blocking injunction' (2017) 28(5) Ent. L.R 171.
[100] Ofcom (n 25).

doms and conflict with the principle of proportionality.[86] It is worth noting that although the same court decided in both cases, it ruled in a different way; while the requested blocking in the first case was considered to be proportionate and in compliance with constitutional rights, the request in the second case was not accepted.

Greece is one of the member states that has implemented in its national law an out-of-court notice and takedown mechanism. According to Article 66E of the Greek Copyright Act 1993, the 'Commission for the notification of online copyright and related rights infringement' is the newly founded administrative authority, responsible for carrying out the proceedings.[87] The new administrative authority issued its first blocking order in 2018,[88] obliging all internet access providers to block 38 infringing websites, including <piratebay.org>. However, it is worth mentioning that this out-of-court procedure shall not apply to cases of infringement committed by end users by means of downloading works or streaming or peer-to-peer exchange of files, or by means of provision of data storing services through cloud computing.[89]

The Commission does not accept the blocking of all future alternative URLs of the already blocked websites on the grounds of lack of precision. Consequently, most of the blocked websites changed their top-level domain and can be accessed again. As Paramythiotis stated, the blocking orders are able to prevent some traffic, but tech-savvy users are still able to have access to illegal content online.[90]

4.3 Blocking injunction in the Nordic countries

Back in 2010, the Danish Supreme Court concluded that the Danish ISP, namely DMT2, was complicit in its users' copyright infringement through the website The Pirate Bay.[91] The court ordered the ISP, through DNS blocking, to prevent its users from accessing the website.

In Finland, the Helsinki Court of Appeals allowed in 2011 a preliminary injunction ordering the intermediary to "discontinue" making available to the public material that infringed copyrights. More specifically, the court ordered the ISP Elisa Oyj to prevent its users from accessing 33 domain names and three IP addresses used by The Pirate Bay, ordering both the techniques of DNS and IP blocking.[92] With the order of IP blocking, as an additional "layer of protection", the Finnish courts went a step further than the Danish courts.[93]

In 2014 the Icelandic courts compelled the ISPs Vodafone and Hringdu to prevent their users from accessing The Pirate Bay as well as the Icelandic torrent website Deildu.[94] The ISPs agreed to block their users' access to The Pirate Bay and Deildu regardless of which domain name the sites are hosted under. In fact, depending on the extensiveness of the blocking, it could be argued that Iceland has one of the most effective blocking regimes compared to the other Nordic countries.[95]

In 2015 the Oslo District Court decided on compelling Norwegian ISPs to prevent their users from accessing certain domain names relating to The Pirate Bay.[96] Based on s. 56(c) of the Norwegian Copyright Act 2013, the court granted the plaintiffs' motion for an injunction, ordering Norwegian ISPs to block access to domain names (DNS blocking) that belonged to The Pirate Bay for a period of five years. This case is of great importance, since it is the first example in Norway of a court ordering ISPs to block access to illegal content available online.[97]

In Sweden, the first blocking injunction in a copyright case was granted by the Swedish Patent and Market Court of Appeal in 2017. In the landmark case of *Universal Music AB v B2 Bredband AB*,[98] the court ordered B2 Bredband AB to block access to The Pirate Bay and Swefilmer for a period of three years. Although the court of the first instance, the Stockholm District Court, rejected an application for an injunction against the Swedish ISP B2 to block access to The Pirate Bay and Swefilmer, the Swedish national coordinator for IP crime, Paul Pinter, called for an amendment in the law. He suggested a considerable number of reforms in order to allow seizure and confiscation of intangible assets during the course of an investigation, to introduce a felony in copyright and trade mark law to provide more clear definitions regarding criminal provisions and lastly, to block sites that infringe copyright or trade mark law.[99] After the suggestions of the national coordinator for IP crimes, the Patent and Market Court of Appeal reversed the first instance decision in 2017, ordering the ISP to block access to The Pirate Bay and Swefilmer.

It is worth noting that it was not until four years ago that the Swedish court granted an injunction against an ISP for the first time. While the other Nordic countries had already allowed blocking injunctions, Sweden is the last country that ordered a blocking injunction.

5. BLOCKING INJUNCTIONS AND COLLATERAL DAMAGE

What will happen if the target website or a specific location within the website share a single IP address with other legitimate websites? In this situation, the ISPs action to block access to a specific infringing website may result in customers being blocked from accessing the other legitimate websites that share the same IP address. As Ofcom characteristically emphasized, each blocking measure also carries a risk of "over-blocking".[100]

There is a number of different techniques that ISPs could use to block access to infringing websites. Two of the most common techniques are DNS blocking and IP address blocking. However, it is very important to mention that both techniques are capable of being circumvented.[101] More specifically, the DNS blocking is more easily circumvented in contrast to the IP address blocking. As it was held in the *Cartier v Sky* case, where the court granted for the first time a blocking injunction to protect trade mark rights, circumvention takes place not only on the part of the users but also by the website operators.[102]

The issue of shared IP addresses was considered in the *Cartier v Sky* case. Justice Arnold, who delivered the judgement, considered the impact that a blocking injunction may have on legitimate websites. In this respect, Justice Arnold considered three possible scenarios.[103] In case that the target website does not share an IP address with other websites, an order that requires IP address blocking would not affect lawful users. Whereas, in case that the target website shares an IP address with other websites which are engaged in unlawful activity, IP address blocking would be appropriate. Last but not least, where a particular target website shares an IP address with other lawful websites, the proper measure would be DNS blocking and not IP blocking.

As far as the first scenario is concerned, one could argue that it is not problematic. When a target website does not share the same IP address with other websites, the technical measure of IP address blocking could accurately target a specific infringing website. Nevertheless, the second and the third scenarios are more problematic and thus require closer examination.

In the second scenario, the target website shares the same IP address with other websites, which according to Justice Arnold are engaged in unlawful activity. In this regard, an order for IP blocking would be appropriate. At this point, more emphasis should be given to the word "unlawful" that was used by the court. The court preferred the word "unlawful" rather than "infringing" activities. The choice of the specific word is very wise. An "unlawful" activity could, for instance, entail material linked to child pornography. In these circumstances, IP blocking was considered as an appropriate measure, since according to the judge's view, there was no collateral damage to any "lawful" activity.

As Roy and Marsoof stated, this means that the reach of a blocking injunction could be much broader than what was anticipated by the two EU instruments, namely the Information Society Directive and the Enforcement Directive.[104]

Although in situations involving unlawful activities, such as child pornography, the landscape is clear for the court to order IP blocking, the problem arises where it is difficult to draw a line between what is lawful and what is not. In these circumstances, it is the applicant that determines and certifies the unlawfulness of the other website and not the court. It is the applicant that has the burden to certify to the court that he/she has sent a notice to the contact address given by the website notifying them about the order and providing them with the opportunity to move to an alternative server or explain why the website is not operating unlawfully.[105] Unfortunately, one could argue that there could be instances where either the contact information of the website operator is not available or the operators cannot be contacted due to technical problems.

In the third scenario, the target website shares the same IP address with other lawful websites. In this situation, courts have preferred to adopt DNS blocking instead of IP blocking so as to avoid collateral damage. More specifically, in the Danish case of *Telenor v IFPI Danmark* and in the Norwegian case *Nordic Records Norway AS v Telenor ASA* the courts held that is much more effective to block access to infringing websites by the adoption of a DNS blocking.[106] However, one should not disregard the limitations of using this technique. For instance, DNS blocking could be easily circumvented via relatively simple measures.[107]

Despite the advantages of using DNS blocking, the possibility of causing collateral damage remains. In cases where both legal and illegal content share the same domain name, a DNS blocking would result in blocking access to everything. Bearing in mind all the possible scenarios, the next step would be to examine the third blocking technique of URL blocking.

In situations where both legal and illegal content share the same IP address or the same domain name, it is the court or the ISP that has to deploy another, less controversial method. The reason why this method is more effective is that the URL blocking precisely targets an infringing website or a specific part of a website. For example, assuming that the infringing content resides in a distinct page of the website C. ISPs could adopt IP blocking, but this would block access to all websites (A,B,C) that share the same IP address. Alternatively, ISPs could adopt DNS blocking by targeting parent domains and block access to the <main-domain.com>. Once again, websites that share the same domain name (B and C for example) would be blocked in their entirety. Moving a step further, if the sub-domain of the website C is blocked (<sub-domain-C.main-domain.com>) that would result in the blocking of the legitimate content as well. By deploying the URL blocking, ISPs would have to block the URL <http://sub-domain-C.main domain.com/infringing.html>. Thus, only the specific part or the website C would be blocked, leaving all other websites that are associated with that domain and share the same IP address intact.[108]

Despite the increased accuracy of URL blocking measures, this method still suffers from serious drawbacks. Circumventing an IP or DNS blocking measure would require the operators to move to a different host or change the domain name which will incur additional costs, while circumvention of a URL blocking measure could be achieved by changing the URL.[109]

Circumvention is a "thorn" in the process of finding the infringing material and blocking access to it. In the UK, the High Court acknowledged that there are circumvention methods which can be used by website operators, including changing IP addresses and URLs. These can be combatted by updating the IP addresses or URLs that are blocked.[110] The so called "notice and block" approach has proved to have positive results to tackle circumvention by the website operators. Although the initial blocking is achieved via a court order, in the event that a website ope-

rator changes the IP address or URL, a subsequent notification that provides the new IP address or the new URL would oblige the ISPs to update their system. Thus, the target website remains inaccessible. Marsoof opines that, at least in the way it is practised in the UK, blocking injunctions are capable of effectively tackling circumvention on the part of website operators.[111]

According to Lodder and Polter,[112] the UK has experienced a considerable decrease of 71.2% in traffic to blocked websites, while the rest of the world has experienced an increase of 27.8%. At the same time, the UK has experienced a sharp increase in traffic to non-blocked websites, in particular 146% compared to the rest of the world that saw an increase of 67.6%. Based on these findings, it is suggested that UK users who have been blocked from accessing websites have not circumvented the blocks but have started using other websites.

In any event, bearing in mind the possible unintended consequences of collateral damage as well as the reality of circumventing blocking orders, courts have to choose the appropriate blocking technique very carefully.

6. RECOMMENDATIONS

Blocking injunctions against ISPs are one of the most valuable remedies that a copyright owner can rely on for the enforcement of IP rights. However, due to the lack of harmonised standards, national courts implement the Information Society Directive differently based on their national laws. This leads to courts in some Member States ordering technology-specific blocking, while courts in other Member States issue an injunction with non-specific technical measures or even do not order ISPs to block infringing websites.

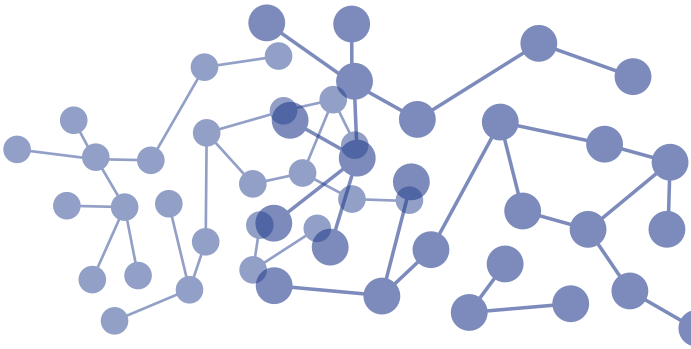
It is notable that countries such as the UK, Belgium and Greece have been issuing blocking injunctions with specific technical measures. More specifically, the UK court in the *Football Association Premier League Ltd v British Sky Broadcasting Ltd* ordered a hybrid method of blocking which included the combination of IP blocking and URL blocking.[113] In Belgium, the Belgian court in the *SABAM v Scarlet* case, ordered a technical expert to conduct a technical evaluation of the filtering applications.[114] In Greece, the Athens Court of First Instance ordered an IP address blocking in order to block access to infringing websites.[115] On the contrary, the Danish courts granted blocking injunctions by ordering the ISPs to take all the necessary measures to prevent access by their customers.[116]

This part will recommend how blocking injunctions could be more effective, through EU harmonisation and it will provide alternative measures on how to tackle online copyright infringement in a more effective way.

6.1 EU harmonisation on the framework of blocking injunctions

As it was outlined in the previous parts, there is no standard practice on the employment of blocking injunctions within the Member States. This generates a debate on whether blocking injunctions granted from the courts should indicate specific technical measures. In *UPC Telekabel*, the court stated that it is the intermediary's responsibility to choose and implement the appropriate technical measures to protect right holders.[117] This responsibility is justified because intermediaries have the knowledge and can adopt the resources available to them. However, this task is not considered to be an easy and straightforward one since the deployment of technical measures has to strike the right balance between the protection of copyrights on the one hand and the freedom to conduct a business and the freedom of information on the other hand.

Although it is understandable that it is within the Member States discretion to define transposition measures, in absence of general guidance from the Commission, intermediaries may not be able to foresee a constructive framework that will strike the right balance between the different rights in question. Due to the lack of a harmonised standard from the Commission, national courts would implement the Information Society Directive differently based on their national legislation.



[101] Centre for Democracy and Technology, ' The Perils of Using the Domain Name System to Address Unlawful Internet Content (13 October 2011) <https://cdt.org/insight/the-perils-of-using-the-domain-name-system-to-address-unlawful-internet-content/> accessed 18 October 2021.

[102] *Cartier v Sky* [2014] EWHC 3354 (Ch); [2015] 1 All E.R. 949 [27].

[103] Ibid [256].

[104] Roy and Marsoof (n 5) 74.

[105] Ibid.

[106] *Telenor v IFPI* (n 91); *Nordic Records Norway AS v Telenor ASA*, Case 10-006542ASK-BORG/04 (9 February 2010, Norwegian Court of Appeal 'Borgarting Lagmannsrett').

[107] Songe-Moller and Foss (n 93) 37.

[108] Roy and Marsoof (n 5) 74.

[109] Ibid.

[110] *Richemont International SA and others v British Sky Broadcasting Ltd and others* [2014] EWHC 3354 (Ch) [27].

[111] Marsoof (n 3) 632.

[112] A. Lodder and P. Polter, 'ISP blocking and filtering: on the shallow justification in case law regarding effectiveness on measures' (2017) 8(2) EJLT <https://ejlt.org/index.php/ejlt/article/view/517> accessed 18 October 2021.

[113] *Football Association Premier League Ltd v British Sky Broadcasting Ltd* [2013] EWHC 2058 (Ch).

[114] *SABAM v SA Tiscali (Scarlet)* (2007) No. 04/8975/A (District Court of Brussels).

[115] Athens Court of First Instance, Case 4658/2012.

[116] *Telenor v IFPI* (n 91).

[117] Judgement of 27 March 2014, *UPC Telekabel* (n 11).

Courts in different Member States have reached different conclusions on the proportionality of blocking orders. This calls for harmonisation of the utilization of appropriate blocking measures by ISPs. It would be rather helpful if the Commission could establish a framework to improve the practicality of effective blocking. Wang suggests that it would be advantageous if the EU could introduce some successful experience from countries such as the USA.[118]

According to the US Copyright Act, for injunctive relief considerations, there is a formal scheme of four criteria.[119] The court will assess the following: first, whether such an injunction (alone or in combination with other injunctions against the same ISP) would significantly burden the provider or the operation of the provider's system or network. Second, the magnitude of the harm likely to be suffered by the copyright owner if steps are not taken. Third, whether the implementation of such an injunction would be technically feasible and effective and would not interfere with access to non-infringing material at other online locations and fourth, whether there are other less burdensome and comparably effective means of preventing or restraining access to the infringing material.

One question remains: should the courts order specific technical means to prevent users from accessing the target website or should it be at the discretion of the ISPs to decide the appropriate technical measure? It is difficult to argue for or against one side. On the one hand, courts will guarantee the legality of the process, bearing in mind the principle of proportionality when trying to strike a balance between the right of the copyright holders, the right to conduct a business and the right of access to information. However, courts do not have the technical knowledge to decide the proper blocking technique. For instance, the court could not be aware of how many websites share the same IP address, when ordering IP address blocking which entails the risk of over-blocking.[120]

On the other hand, ISPs have the technical knowledge and the resources to choose and implement the most appropriate technical measure. What they lack is the position to balance and guarantee the legitimate interests of the involved parties. Thus, it would be ideal if there is a combination of court protection and technical expertise. Before courts decide and order a specific blocking injunction, there should be communication and collaboration with technical experts. In this situation, every blocking injunction would be the result of technical knowledge and within the judicial proceedings.

In this context, it is crucial to mention the "notice and block" regime adopted by the UK, in view of potential circumvention techniques. In the UK, although the initial blocking of a target website is achieved via the court process, in the event of changing the IP address or URL by the operators of the website, there is a subsequent notification providing the new IP or URL that obliges the ISP to update its system, so that the target website remains inaccessible.[121] It is obvious that through this process, right holders seek a blocking injunction under the auspices of the court and at the same time, in the event of circumvention, they are advised to notify the ISP directly in order to update its system.

Following the example of the UK, the EU Member States should adopt a "notice and block" regime. The copyright owners should initially seek a blocking injunction through the court process, which will safeguard their rights. With the aid of a technical expert, the court would decide and order the most appropriate blocking technique. However, in the event of a potential circumvention, right holders should not be left unprotected or should not be obliged to initiate proceedings from the beginning. A subsequent notification to the ISP regarding the new "landscape" would save time and would be cost effective.

6.2 Alternative measures on how to tackle online copyright infringement

To tackle online copyright infringement more effectively, it is believed that blocking injunctions alone are not the best line of action. It would be efficient if there are online legal alternatives and sufficient information to the general audience regarding the rationale of intellectual property.

More specifically, the successful operation of services such as Spotify and Netflix results in a significant decline in online infringement.[122] If users have at their disposal legal alternatives with low cost, they will choose to subscribe and access the legal content instead of searching online for websites that may provide access to the content in question. In addition, according to Ofcom the time between the premiere of a series or movie and the actual time that users can access the content is very important.[123] For instance, in the UK, Sky has exclusive licensing agreements with all the major US studios for the premieres of their movies.[124] After their cinema release, the titles are available via Sky broadcast TV channels and Over the Top (OTT) service Now TV within at least one year.

Moreover, delisting of infringing websites from search engines could be an effective measure, since it makes it more difficult for users to find unlawful sites.[125] While the website operator can move to an alternative IP address, URL or domain name, if it cannot be secured that there will be a listing for the new location on search engines, then it will be harder for users to find the website. At the same time, users can easily locate lawful alternatives, as they will appear higher in the search rankings.

7. CONCLUSION

To assess the effectiveness of blocking injunctions, one should examine how national courts respond to them. Although the selected jurisdictions have granted blocking injunctions for online copyright infringement, it is evident by the case law that each country had its own starting point for the implementation of this method. Characteristic examples are the UK and Greece, where blocking injunctions have been granted since 2011 and 2012, respectively. On the contrary, Sweden is among the countries that have recently started to issue blocking injunctions.

Apart from the difference in the timing of implementation, another difference lies in the alternative ways of copyright protection. In Greece, for instance, there is the traditional judicial path on the one hand, and the out-of-court notice and take down legal mechanism, through a newly founded administrative authority on the other. This

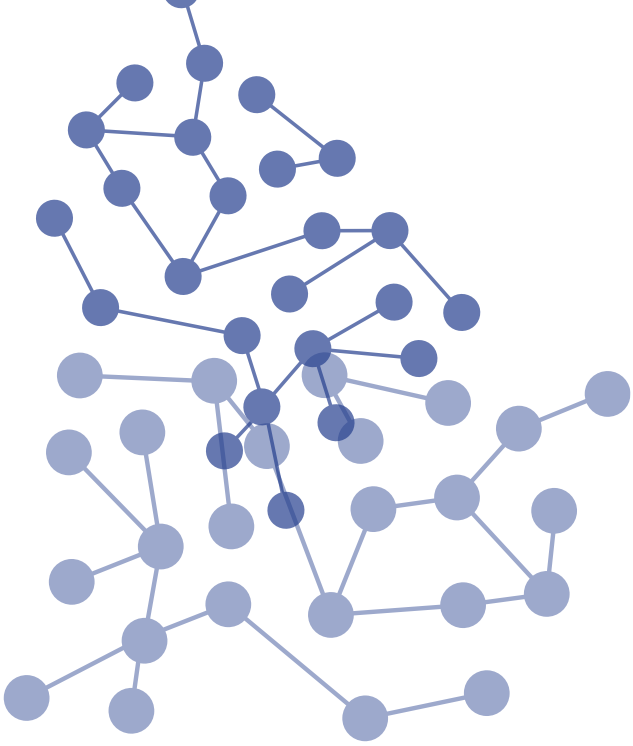
initiative will be very helpful for the right holders, bearing in mind the caseload and slow disposition of cases in the Greek courts.

Without a doubt, website blocking injunctions are a common and valuable method used to prevent unauthorized access to protected works in the online environment. As it is burdensome for copyright owners to identify and initiate proceedings against the users and the website operators, ISPs can easily identify a particular infringing website. From an economic point of view, it is more efficient to require intermediaries to take action to prevent infringement from being committed through their services.

Nevertheless, one should not disregard the concerns that were raised in the previous parts. The fact that Member States in the EU and the UK interpret and deploy blocking injunctions differently, along with the technical issue of who will determine and deploy the blocking injunctions result in ineffective outcomes. In addition, the "shadows" of potential collateral damage and circumvention worsen the situation even more.

Due to the lack of harmonized standards, it is recommended that EU harmonization could enable blocking injunctions to be more effective. It would be rather helpful if the European Commission could establish a framework to improve the practicality of effective blocking. Additionally, it would be ideal if courts and technical experts collaborated before issuing a blocking order. In order to mitigate the circumvention risk, Member States can follow the 'notice and block' regime adopted by the UK. Meanwhile, as the paper focused on online copyright infringement, it provided alternative measures on how to tackle online copyright infringement in a more effective way, by the use of online legal alternatives.

In a report prepared for Ofcom, it was characteristically stated that "no single enforcement solution is likely to address online copyright infringement in isolation; a complementary mix of measures including better lawful alternatives, more education about copyright matters, and targeted enforcement is more likely to be successful".[126]



Despoina Farmaki

Despoina Farmaki is currently a PhD candidate in Law at Brunel University London. Her research focuses on copyright and internet law in the video game industry. She is also a Lecturer at Brunel University London Pathway College, AFHEA, Research Assistant at Brunel University and a member of the Centre for Artificial Intelligence. Despoina holds an LLM in International Commercial Law from Brunel University (2019) and is a Greek qualified lawyer since 2018. She obtained her bachelor's degree in law (LLB) in Greece.

[118] F. Wang, 'Site-blocking Orders in the EU: Justification and Feasibility' (2014) 14th Annual Intellectual Property Scholars Conference, Boalt Hall School of Law, University of California, Berkeley, 7-8 August 2014.

[119] Copyright Law of the United States (Title 17) 1976, s. 512 (j)(2)(A-D).

[120] L. Feiler, 'Website Blocking Injunctions under EU and U.S Copyright Law – Slow Death of the Global Internet or Emergence of the Rule of National Copyright Law?' (2012) TTLF Working Paper No.13 < https://law.stanford.edu/wp-content/uploads/sites/default/files/publication/203758/doc/slspublic/feiler_wp13.pdf> accessed 18 October 2021.

[121] Marsoof (n 3) 632.

[122] Copia, 'The carrot or the stick?' (8 October 2015) <https://copia.is/library/the-carrot-or-the-stick/> accessed 18 October 2021.

[123] IDATE Consulting, 'Online content study: changes in the distribution, discovery and consumption of lawful and unauthorised online content' MC 359 Final Report (November 2015) <https://www.ofcom.org.uk/__data/assets/pdf_file/0031/69196/online-content-study-010316.pdf> accessed 18 October 2021.

[124] Ibid.

[125] Ofcom (n 25).

[126] Kanter Media, ' OCI Tracker: High volume infringers analysis report' 3 <http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/online-copyright/w4/HIGH_VOLUME_INFRINGERS.pdf> accessed 2 November 2021