IIC (2015) 46:632–664
DOI 10.1007/s40319-015-0379-z

ARTICLE

The Blocking Injunction – A Critical Review of Its Implementation in the United Kingdom Within the Legal Framework of the European Union

Althaf Marsoof

Published online: 1 September 2015

Abstract This article critically evaluates the manner in which the blocking injunction has been implemented in the United Kingdom, the legal basis for which is derived from the legal framework of the European Union. Unlike the extrajudicial and privatised Notice and Takedown ("N&T") process, the blocking injunction is a court-supervised mechanism and, hence, avoids the key criticism levelled against N&T. Yet, there are problems with the blocking injunction, in particular the manner in which it is implemented. This article first demonstrates that, unlike in the context of copyright enforcement, the legal basis for the blocking injunction in the field of trademark protection is suspect. Secondly, the article posits that the procedure pertaining to the grant of a blocking injunction runs counter to the principles of natural justice – in that neither the relevant EU directives, nor their domestic implementations, provide for the target website operators (i.e. the authors of online content), whose content is sought to be blocked, to be notified of, or joined in, the proceedings where injunctions are sought. As such, it is argued that an important safeguard that has been incorporated into blocking orders, which allows affected parties to apply for a variation or vacation of a blocking order, is rendered meaningless. Lastly, the article identifies four areas – i.e. circumvention, multiplicity of proceedings, barriers to legitimate trade and costs of implementation – where there might be problems in the future that may question the efficacy of this remedy.

Keywords Blocking injunctions · Internet service providers · IP enforcement · Natural justice · Circumvention · Multiplicity of proceedings · Costs of implementation

A. Marsoof (✉)
Ph.D. candidate
The Dickson Poon School of Law, King's College London, London, UK
e-mail: althaf.marsoof@kcl.ac.uk

1 Introduction

For many years, it was the Notice and Takedown ("N&T") approach that allowed intellectual property ("IP") owners aggrieved by the presence of infringing online content to have such content removed (or "taken down") from the internet in an expeditious and cost-effective way by notifying the relevant internet intermediaries that are responsible for making the content visible to internet users. Today, most intermediaries have N&T policies. Upon closer scrutiny, it becomes apparent that the emergence of N&T is a direct consequence of law reform. Thus, in the United States, the Digital Millennium Copyright Act 1998 ("DMCA") introduced Sec. 512 into Title 17 of the US Code providing a safe harbour to internet intermediaries against claims for damages in the event they expeditiously take down, or remove links to, content that infringes copyright upon acquiring knowledge of an infringement. Such knowledge is usually imputed through a takedown notice, thus giving birth to N&T in the US. Similarly, the Electronic Commerce Directive of the European Union[1] (Arts. 12–15) has created a safe harbour that incentivises EU-based intermediaries to implement N&T policies to tackle illegal content.

A criticism levelled against N&T relates to the fact that determinations made by online intermediaries, pertaining to the legality or otherwise of content, are influenced by their own potential liability that could be imposed under the legal framework within which they operate. That is, the immediate removal of content subject to a takedown notice is the most assured way for these intermediaries to avoid liability, such liability being premised on their failure or omission to act consequent to acquiring knowledge of infringing material on their platforms. Thus, it is alleged that these intermediaries, when removing content that they *believe* is illegitimate, act in their own best interest, although there is a real possibility that even legitimate content may be removed in the process. This over-cautious attitude of intermediaries towards N&T and the lack of an independent, unbiased and balanced mechanism by which a determination as to the legality of content can be reached is the central problem that taints N&T.

It is in this setting that a new approach is gaining popularity in the EU, where aggrieved IP owners can apply to a court seeking an injunction to compel internet service providers ("ISPs") to block access to infringing websites ("target websites") – popularly known as the blocking injunction. Since in any given jurisdiction there are only an identifiable number of ISPs, a blocking injunction targeting all ISPs enables right-holders to seek an effective remedy to curb the effects of infringing content. Especially when foreign intermediaries host infringing content, making it difficult to control their conduct through domestic court proceedings, the blocking injunction becomes a pragmatic solution.

This article engages in a critical review of the blocking injunction as a tool for the protection and enforcement of IP rights, with specific focus on developments that have taken place in the recent past in the United Kingdom within the larger

[1] 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 ("Electronic Commerce Directive").

legal framework of the European Union. In terms of structure, the article first scrutinises the legal basis for blocking injunctions and argues that the legal basis for injunctions in the field of trademark protection is problematic. In the second part, the article considers whether the implementation of the remedy in the UK, which also incorporates certain safeguards, complies with the principles of natural justice. Lastly, some of the practical aspects of the blocking injunction are considered.

2 The Legal Basis for the Blocking Injunction

While N&T applies to content-hosts and search engines, compelling them to take down or de-link alleged infringing content hosted or linked by them, the blocking injunction has been used in the EU to control the conduct of ISPs, compelling them to block access to alleged infringing content.

2.1 The Copyright Context

It was in the copyright context that blocking injunctions were first used in the EU to protect against copyright infringements. This was made possible after 2001 owing to the Information Society Directive,[2] which in Art. 8(3) obligates EU Member States to ensure that aggrieved parties are permitted to seek injunctions against internet intermediaries, with a view to mitigating the effects of online copyright infringements. Article 8(3) of the Information Society Directive has been implemented in EU Member States – in the UK by the addition of Sec. 97A (and Sec. 191JA in respect of performers' rights) to the Copyright Designs and Patent Act 1988 ("CDPA"), which provides that the High Court of England and Wales shall have the power to grant an injunction against a "service provider",[3] where that service provider has actual knowledge of another person using its service to infringe copyright.

It is noteworthy that the scope of this provision is not only wide enough to take into consideration the infringements of persons with whom a service provider has a contractual relationship (e.g. subscribers), but also any other "person *using the service* to infringe copyright". In the UK, blocking injunctions against ISPs are premised on this statutory provision, which illuminates the breadth of the provision – as it cannot be said that UK-based ISPs have any link, contractual or otherwise, with the individuals who maintain and operate foreign websites that host or link infringing content, such persons often residing in jurisdictions outside the EU. More importantly, it cannot be contended that ISPs that merely provide internet access

[2] 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 ("Information Society Directive").

[3] The term "service provider" has the meaning given to it by Regulation 2 of the Electronic Commerce (EC Directive) Regulations 2002, which transposes the Electronic Commerce Directive into the laws of the UK. Accordingly, a service provider means any "information society service" and includes ISPs, content-hosts and search engines.

engage in any form of copyright infringement – they neither authorise nor encourage another's copyright infringement.

It is also noteworthy, in the UK context, that injunctions are available only against service providers that have "actual knowledge" of the underlying infringements, although this requirement is not contained in Art. 8(3) of the Information Society Directive itself. It appears that the inclusion of this requirement was possible because Recital 59 of the Information Society Directive provides that "conditions and modalities relating to such injunctions should be left to the national law of Member States".[4] Although such knowledge is capable of being imputed upon a proper notice being served on the service provider,[5] it is unclear as to why the UK Government decided to impose such a requirement. After all, it does not stand to reason to compel a right-holder to first notify an ISP before resorting to the court system to seek a blocking injunction, especially since the requirement of knowledge on the part of an ISP (unlike other types of intermediaries such as content-hosts, search engines and services that cache content) is not capable of sustaining a claim for damages in view of the ISP's failure to take action to block access to the infringing material.[6] Perhaps the only reasonable explanation, therefore, for the existence of such a knowledge requirement is that it allows an ISP to investigate a right-holder's claim,[7] although even in relation to a credible claim, it is unlikely that the ISP would take any positive steps to address the interests of the right-holder.

Nevertheless, in view of the knowledge requirement under UK law, it is only upon an ISP being served with a notice detailing the specific particulars of target websites, that an aggrieved party may seek the assistance of the High Court in compelling the ISP to block access to those websites. Such a blocking injunction is not contrary to the limitation of liability provisions in the EU's Electronic Commerce Directive (i.e. Art. 12),[8] as although a claim for damages does not lie against ISPs, it does not mean that they are exempt from injunctions, such as blocking injunctions.[9] Thus, the blocking injunction against ISPs takes the form of a "notice and block" regime.

In the UK, copyright owners have sought blocking injunctions in a number of instances. *Twentieth C. Fox v. BT* was the first in a series of cases where a blocking injunction was issued under Sec. 97A of the CDPA. This was a sequel to an earlier dispute between the well-known film production company Twentieth Century Fox and Newzbin Ltd., where the latter maintained a website at the URL http://www.

[4] Headdon (2012), p. 141.

[5] CDPA, Sec. 97A(2).

[6] This becomes clear upon a reading of Art. 12 of the Electronic Commerce Directive.

[7] At least, this was Arnold J's explanation in *Twentieth Century Fox* et al. *v. British Telecom Plc* [2011] *EWHC* 1981 (Ch) ("*Twentieth C. Fox v. BT*"), para. 141.

[8] *See* Electronic Commerce Directive, Art. 12(3): "This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, *of requiring the service provider to terminate or prevent an infringement*" (emphasis added).

[9] *But see* discussion under the heading "The Trademark Context" (immediately below).

newzbin.com resulting in large-scale infringement.[10] Upon the High Court issuing an injunction against Newzbin to cease operations, an unknown third party restored the website from an offshore location – making it impossible for Twentieth C. Fox to seek redress via the court process against that unknown party. Thus, adopting a different strategy, Twentieth C. Fox filed an action against British Telecom, an ISP operating in the UK, seeking an injunction compelling the latter to block access to the infringing website. Justice Arnold, delivering the judgement of the High Court, issued a blocking injunction resulting in UK internet users being prevented from accessing the infringing website – thus mitigating the impact of copyright infringement within the UK, despite the operators of the infringing website moving to an offshore location outside the EU.

Following *Twentieth C. Fox v. BT*, blocking injunctions were issued in subsequent cases, such as *Dramatico v. Sky*,[11] *EMI Records v. Sky*,[12] *Football Association v. Sky*[13] and *Paramount Entertainment v. Sky*,[14] where injunctions were issued to prevent the infringement of copyright. It is noteworthy that in all these cases it was Arnold J who ordered the blocking injunctions.

2.2 The Trademark Context

While blocking injunctions have been dominated by claims in the field of copyright, it was not until as recently as 2014 that a blocking injunction was issued in the trademark context. Thus, in *Richemont v. Sky*,[15] a blocking injunction quite similar to those issued under the copyright regime was issued against five major UK-based ISPs in order to block access to certain identified counterfeit websites that infringed trademark rights. Unlike in the copyright context, however, there "is no statutory counterpart in the field of trade marks to section 97A [of the CDPA]".[16] Justice Arnold, delivering the judgement of the High Court, overcame this shortcoming by relying on Sec. 37 of the Senior Courts Act 1981 ("SC Act"), which empowered the High Court to issue injunctions, by adopting the following principle established in *Norwich Pharmacal Co v. Customs & Excise Commissioners*:

> If a man has in his possession or control goods the dissemination of which, whether in the way of trade or, possibly, merely by way of gifts (see *Upmann v Forester*, 24 Ch.D. 231), will infringe another's patent or trade mark, he

[10] *See Twentieth Century Fox et al v. Newzbin Ltd* [2010] *EWHC* 608 (Ch) ("*Twentieth C. Fox v. Newzbin*").

[11] *Dramatico Entertainment Ltd v. British Sky Broadcasting Ltd* [2012] *EWHC* 268 (Ch) ("*Dramatico v. Sky*").

[12] *EMI Records Ltd v. British Sky Broadcasting Ltd* [2013] *EWHC* 379 (Ch) ("*EMI Records v. Sky*").

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

[14] *Paramount Home Entertainment International Ltd v. British Sky Broadcasting Ltd* [2013] *EWHC* 3479 (Ch) ("*Paramount Entertainment v. Sky*").

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

[16] *Richemont v. Sky*, para. 5.

> becomes, as soon as he is aware of this fact, subject to a duty, an equitable duty, not to allow those goods to pass out of his possession or control at any rate in circumstances in which the proprietor of the patent or mark might be injured by infringement ensuing. […] This duty is one which will, if necessary, be enforced in equity by way of injunction.[17]

Thus, building on this, Arnold J observed:

> … it is not a long step from this to conclude that, once an ISP becomes aware that its services are being used by third parties to infringe an intellectual property right, then it becomes subject to a duty to take proportionate measures to prevent or reduce such infringements even though it is not itself liable for infringement.[18]

In addition, given the novel ways in which the High Court's Sec. 37 jurisdiction has been previously exercised, Arnold J was satisfied that the High Court possessed the power to issue a blocking injunction against the ISPs as requested in *Richemont v. Sky*.[19]

Despite the broad language of Sec. 37 of the SC Act, however, Arnold J was of the view that the discretionary powers of the High Court to issue injunctions must be interpreted consistently with EU law,[20] in particular with Art. 11 of the Enforcement Directive,[21] which applies to the enforcement of IP rights, including trademarks.[22] Article 11 (third sentence) provides that: "Member States shall also ensure that rightholders are in a position to apply for an *injunction against intermediaries whose services are used by a third party to infringe an intellectual property right*."[23]

Thus, in the context of *Richemont v. Sky*, the blocking injunction was granted against Sky and the other ISPs on the basis that the threshold factors in a typical CDPA Sec. 97A case were satisfied. Accordingly, Arnold J concluded that since the ISPs were: (1) intermediaries, (2) the operators of the identified counterfeit websites were engaging in trademark infringement, (3) the operators of the counterfeit websites were using the ISPs' services to commit the infringements, and (4) the ISPs had actual knowledge of the infringements, it was justifiable for a blocking injunction to be issued in the circumstances of the case.

[17] [1974] *AC* pp. 133, 145–146.

[18] *Richemont v. Sky*, para. 135.

[19] *Richemont v. Sky*, para. 107.

[20] *Richemont v. Sky*, para. 140.

[21] *See* Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights ("Enforcement Directive").

[22] But Art. 8(3) of the Information Society Directive deals exclusively with the enforcement of copyright through injunctions against intermediaries and the Enforcement Directive's corresponding provision does not prejudice the operation of Information Society Directive in respect of this (*see* Enforcement Directive, Recital 23 and Art. 11 (third sentence)). Thus, the Information Society Directive is *lex specialis* in relation to the Enforcement Directive.

[23] Emphasis added.

It is convenient to consider the last threshold factor which imposes a knowledge requirement first. In this regard, it must be noted that Art. 11 of the Enforcement Directive, which is applicable to the trademark context, does not impose a "knowledge" requirement. Further, since the UK Government did not specifically choose to transpose Art. 11 of the Enforcement Directive into UK law, on the basis that the existing legal framework already provided for such injunctions, there was nothing in the domestic context that required the knowledge requirement to be incorporated into the equation of a blocking injunction in the trademark context. The mere fact that the CDPA's Sec. 97A added a knowledge requirement does not necessarily point in favour of such an addition in other areas of IP protection. However, Arnold J saw fit to read the knowledge requirement into the trademark context, in view of the fear that failure to do so would amount to imposing a general monitoring obligation on the part of ISPs contrary to Art. 15 of the Electronic Commerce Directive: "If ISPs could be required to block websites without having actual knowledge of infringing activity, that would be tantamount to a general obligation to monitor."[24]

Yet, it is unclear as to how this conclusion was reached. If ISPs were immune from claims for damages in terms of Art. 12 of the Electronic Commerce Directive, then the mere acquisition of knowledge of an underlying infringement would not suffice to render an ISP liable for damages under substantive law. In view of the safe harbour conferred on ISPs, there is no reason to believe that the lack of a knowledge requirement would result in the imposition of a general monitoring obligation. In any case, since ISPs do not become obligated to block access to identified infringing websites unless a court orders them to do so (failure leading to contempt), the knowledge requirement seems a rather redundant introduction. In addition, Arnold J's own conclusion that an ISP may be supplied with knowledge, in addition to being notified by right-holders, "as a result of being served with […] evidence in support of the […] application [seeking a blocking injunction]",[25] supports this view. For the foregoing reasons, it would have been prudent for Arnold J to have sought a clarification from the Court of Justice of the EU ("CJEU") on whether the knowledge requirement should apply in circumstances where the implementing EU Member State had decided not to expressly provide for such a requirement by enacting legislation.

On the other hand, although there was no doubt that the first and second threshold factors were satisfied, Arnold J's reasoning as regards the third threshold factor – i.e. whether the counterfeit website operators "use the ISPs' services to infringe" – requires further analysis, especially in view of the notable differences in the way copyright and trademark infringements are committed.

To begin with, none of the defendant ISPs had any contractual relationship with the individual counterfeiters, thus lacking contractual control over them. Nor did these ISPs have any technical control over the operation of the target websites. It is quite evident that the role of ISPs, vis-à-vis the service providers that actually *hosted* the target websites (the content-hosts), was far removed from the conduct of

[24] *Richemont v. Sky*, para. 141.

[25] *Richemont v. Sky*, para. 157.

the counterfeiters. Considered this way, is it reasonable to have concluded that the operators of the target websites used "the ISPs' services to infringe" trademark rights?

Justice Arnold's approach in concluding that this condition was satisfied was influenced by EU jurisprudence. He relied on two cases, which were both Austrian references to the CJEU raising questions in the context of copyright. Thus, in *LSG v. Tele2*[26] the claimant, which enforced the rights of music producers and artists, applied for a court order against Tele2 (an Austrian ISP) seeking information about its subscribers in order to file action against perpetrators that engaged in copyright infringement through the use of file-sharing software. It was in this context that the CJEU was called upon to rule on the question whether ISPs were "intermediaries", which the CJEU answered in the affirmative.[27] However, there was really little dispute whether ISPs were intermediaries and it is unclear as to how this ruling of the CJEU provided any assistance as regards the question whether the operators of the target websites *used the services* of the ISPs to infringe trademark rights. In any case, *LSG v. Tele2* concerned the use of file-sharing software on the part of a subclass of Tele2's subscribers to infringe the claimant's copyright.[28] Thus, in *LSG v. Tele2* the conclusion that the ISP's services were being used to infringe copyright could be more easily reached, as some of Tele2's subscribers themselves were engaging in unlawful file-sharing.

The second case relied upon by Arnold J was *UPC Telekabel v. Constantin Film*,[29] which was more relevant to the question that was being considered. In this case, the claimants were the owners of copyright in films which were being made available to the public without the claimants' consent on a website bearing the URL http://www.kino.to. The claimants applied to an Austrian court seeking an order compelling Telekabel, an ISP, to block access to http://www.kino.to. On appeal, the Austrian Supreme Court made a reference to the CJEU on the question whether "a person who makes protected subject matter available on the internet without the rightholder's consent […] is *using the services of the access providers*".[30] The CJEU ruled as follows:

> Accordingly, given that the internet service provider is an inevitable actor in any transmission of an infringement over the internet between one of its customers and a third party, since, in granting access to the network, it makes that transmission possible, it must be held that an internet service provider, such as that at issue in the main proceedings, *which allows its customers to access protected subject-matter made available to the public on the internet by a third party is an intermediary whose services are used to infringe a copyright*.[31]

[26] *LSG-Gesellschaft v. Tele2* (Case C-557/07) [2009] *ECR* I-1227 ("*LSG v. Tele2*").

[27] *LSG v. Tele2*, para. 46.

[28] *LSG v. Tele2*, para. 19.

[29] *UPC Telekabel v. Constantin Film* (Case C-314/12) [2014] *Bus LR* p. 541 ("*UPC v. Constantin*").

[30] *UPC v. Constantin*, para. 23.

[31] *UPC v. Constantin*, para. 32 (emphasis added).

Consequently, Arnold J extended the CJEU's ruling to the context of trademarks:

> … the operators of the Target Websites are infringing the Trade Marks by placing on the internet advertisements and offers for sale which are targeted at UK consumers. The ISPs have an essential role in these infringements, since it is via the ISPs' services that the advertisements and offers for sale are communicated to 95 % of broadband users in the UK.[32]

However, Arnold J's approach is not without problems. In *UPC v. Constantin* the underlying claim concerned the claimants' right to make copyright work *available to the public*. Copyright infringement in that scenario was dependent upon protected material being made available to the public, which was only possible if internet users had access to the website containing the infringing content. Thus, by streaming the films in which copyright subsisted via http://www.kino.to, an exclusive right vested in the claimants was being infringed. It is in this light that ISPs, such as Telekabel, provided their subscribers (no doubt constituting part of the public) access to http://www.kino.to, thereby making the copyright material available to the public. Thus, it was possible for the CJEU to conclude that the ISP's service was quintessential for the infringement to occur.[33] The question whether the services of an ISP were being utilised to engage in the underlying copyright infringements was also raised in an Irish case, where *inter alia* an order was sought to block "The Pirate Bay" website at the URL http://www.priratebay.org. Justice Charleton observed in this regard:

> In the context of the detailed description of peer-to-peer copyright piracy in this judgment, I ask myself the question, *whether internet facilities such as those sold by UPC* [*as ISP*] *are being used to infringe the copyright in works owned by the recording company. In the present, though intermittent, sense they are. Each time someone downloads a work from other peer-to-peer users, the facilities of UPC are then being used to infringe the copyright owned by the recording company.* This is a process that for the theft of music takes only seconds, or in the case of a film, some minutes. In a digital sense, that material can then be argued to be on the network of UPC.[34]

Thus, an analysis of the above cases, all of which took place in the copyright context, reveals that the users of ISPs, just like the operators of infringing websites, commit copyright infringement. In other words, while the making of copyright content available on websites for public access, without the authority of the right-holders, by itself is an infringement on the part of the operators of those websites, when an ISP's subscriber makes use of its services to access and download copyrighted content, such an individual act constitutes a separate and independent act of infringement. Accordingly, in the copyright context, there is no room for

[32] *Richemont v. Sky*, para. 155.

[33] *UPC v. Constantin*, para. 32.

[34] *EMI Records* (*Ireland*) *Ltd and others v. UPC Communications Ireland Ltd* [2010] *IEHC* p. 377, para. 99 ("*EMI Records v. UPC*") (emphasis added).

doubt that the services of an ISP against which a blocking injunction is sought are, both directly and indirectly, being used to commit infringement.

Of course, the question may be asked: what if an internet user downloads copyright material for a use that is covered by one of the exceptions provided under Art. 5 of the Information Society Directive (e.g. private use)? In those circumstances, could it be said that an ISP's services are being used to commit an infringement? Obviously, if a copyright exception does apply, then the acts concerned do not infringe any copyright. However, what must be emphasised here is that those exceptions are applicable only in relation to acts "which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder".[35] Thus, for example, in the case of copying for private use, copies can only originate from a source that is itself lawful and does not infringe copyright. In other words, copies can be made only from a lawfully obtained copy.[36] When copyright material (e.g. music and movies, etc.) is made available or indexed on websites without the consent of the right-holders, an internet user downloading such content, even for private use, is not covered by the private-use exception, since the source is unlawful. Accordingly, in all instances where an ISP's users gain access and download copyright material from websites that infringe copyright, it is doubtful that any of the exceptions would apply to such internet users. In the circumstances, there is no doubt that in every single instance when an ISP's subscriber gains access and downloads copyright material from an unauthorised website or online location, the ISP's services are being used to commit an infringement.

In contrast to copyright infringement, trademark infringement takes place in a vastly different manner. An infringement of a protected trademark occurs the moment an unauthorised third party makes *use* of a registered mark in the course of trade and in relation to identical or similar goods or services for which a claimant's mark is registered.[37] The mere *use* of a registered mark in online promotional material (e.g. a paid advertisement on Google or product listing on eBay) would suffice to constitute an infringement. Trademark infringement does not depend on whether an advertisement comprising a protected trademark is communicated to the public, although the infringement would only become a problem to right-holders if it were. Thus, when counterfeiters utilise registered trademarks to design websites or online content, that act alone constitutes an infringement. In other words, the role played by ISPs in providing internet access to their subscribers, upon which of course a subscriber may come across counterfeit websites, does not in any way relate to the infringing acts of the counterfeiters. Moreover, it cannot be concluded that an internet user, who makes a purchase of counterfeit goods via a website, infringes trademark rights, as purchasers of counterfeit goods are often victims, and not perpetrators, of trademark infringement. In addition, and in common

[35] Information Society Directive, Art. 5(5).

[36] *ACI Adam BV and Others v. Stichting de Thuiskopie, Stichting Onderhandelingen Thuiskopie vergoeding* (Case C-435/12) (unreported). *See also* CJEU Press Release No. 58/14 (10 April 2014).

[37] *See* Art. 5 of Directive 2008/95/EC of the European Parliament and of the Council of 22 October 2008 to approximate the laws of the Member States relating to trade marks (Codified version) ("Trade Mark Directive").

circumstances, where a website or content promoting the sale of counterfeits is hosted and operated in a country other than the one in which the ISPs against whom blocking injunctions are sought, it could not be argued that the operators of the target websites had utilised the services of the ISPs in question to commit trademark infringement. There is neither a contractual nor a technical link. Thus, unlike in the copyright context, it cannot be easily concluded that the counterfeiters who operate websites promoting the sale of counterfeit goods use the services of an ISP to commit an infringement.

In a recent article by Husovec and Peguera published in this journal, the authors cited para. 34 of the CJEU's judgement in *UPC v. Constantin* in order to suggest that it is sufficient that the intermediary against whom an injunction is sought is "capable of serving as a communication channel for the infringements", although there need not be a contractual link between the ISP and the alleged infringers.[38] In order to come to this conclusion, the CJEU made use of Recital 59 of the preamble to the Information Society Directive, which provides as follows: "without prejudice to any other sanctions and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary *who carries a third party's infringement of a protected work or other subject-matter in a network*".[39]

On that basis the CJEU came to the conclusion that

> Article 8(3) of [the Information Society Directive] 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 […] is using the services of the internet service provider of the persons accessing that subject-matter, which must be regarded as an intermediary within the meaning of Article 8(3).[40]

Yet, any use of the ISP's services is only indirect, derived from the use made by the ISP's own subscribers who access the infringing content. Thus, it was the broader language utilised in Recital 59 of the Information Society Directive that allowed the CJEU in *UPC v. Constantin* to overcome the narrowness of Art. 8(3).

However, in stark contrast to Recital 59 of the Information Society Directive, Recital 23 of the Enforcement Directive (applicable to trademarks) merely provides that injunctions must be made available "against an intermediary whose services are being used by a third party to infringe the rightholder's industrial property right". This is precisely what is found in the third sentence of Art. 11. Thus, insofar as the Enforcement Directive is concerned, it is not sufficient that the ISP concerned merely carries a third party's infringement. An ISP's services must be *used for the infringement*, which is much narrower language. In the circumstances, the conclusion reached by the CJEU in *UPC v. Constantin*, which interpreted the Information Society Directive in the context of copyright infringement, cannot be applied to the trademark context under the Enforcement Directive.

[38] Husovec and Peguera (2015), p. 13.

[39] Information Society Directive, Recital 59 (third sentence) (emphasis added).

[40] *UPC v. Constantin*, para. 40.

There is an additional argument that potentially supports this view, in relation to which reference must be made to the Electronic Commerce Directive. Although the remedies available against ISPs are limited under Art. 12(1) of that directive, Art. 12(3) provides that "[t]his Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of *requiring the service provider to terminate or prevent an infringement*".[41] Obviously, injunctions are typically envisaged by this provision. Yet, notably, an ISP can only be required to *terminate or prevent an infringement* from occurring. A blocking injunction in the copyright context achieves precisely this – by ensuring that an ISP's own users do not gain access to infringing websites. In other words, a blocking injunction compels an ISP to ensure that no infringement takes place on the part of its own users. This not only terminates existing infringements but also prevents future infringements from occurring. However, this is not what happens in the trademark context. Blocking access to counterfeit websites does not *prevent* any infringement as such. This is because the existence of a trademark infringement is independent of the conduct of an ISP's own users. All that happens is that the ISP, by blocking access to the source of trademark infringement, merely prevents internet users in the country in which it operates from *accessing* the source of infringement. This is clearly not the same as terminating or preventing an infringement, which in this context could only be done if the infringing content is removed at the very source. Therefore, since the blocking injunction issued against ISPs in the trademark context by no means *terminates* or *prevents* the infringement from occurring, it cannot be a remedy envisaged under Art. 12(3) of the Electronic Commerce Directive. If this were true, it may even be the case that blocking injunctions cannot be issued against ISPs in the trademark context, in view of the general immunity that Art. 12(1) of the Electronic Commerce Directive otherwise provides. Thus, there is a link between an intermediary's ability to *terminate* or *prevent* an infringement and whether its services are being used for the infringement – that is, only if its services are being used for the infringement is it possible for it to prevent the infringement from occurring. Thus, unlike in the copyright context, since ISP users themselves do not engage in trademark infringement, it is difficult to argue that the ISP's services are being used for the trademark infringement or that ISPs are capable of terminating or preventing the trademark infringement from occurring.

There is, however, one consequential point that needs to be addressed, which relates to the CJEU's ruling in *L'Oreal v. eBay*.[42] One of the questions referred to the CJEU was:

> … whether, for the proprietor of a trade mark registered in a Member State of the EU or of a Community trade mark to be able to prevent, under the rules set out in Article 5 of [the Trade Mark Directive][…], the offer for sale, on an online marketplace, of goods bearing that trade mark which have not previously been put on the market in the EEA or, in the case of a Community

[41] Emphasis added.

[42] *L'Oreal SA and others v. eBay International and others* (C-324/09) [2011] *ECR* I-06011 ("*L'Oreal v. eBay*").

> trade mark, in the EU, it is sufficient that the offer for sale is targeted at consumers located in the territory covered by the trade mark.[43]

In short, where both the conduct of an infringer and the infringing goods originate in a third state, the question posed was whether a trademark infringement is committed within the EU, entitling a trademark owner to prevent such unauthorised use of a trademark, if an online offer targets consumers in an EU Member State. The CJEU's response was in the affirmative.[44] Although this question was posed in the context of product listings in an online marketplace, it could be extended to websites and other online material that incorporate trademarks. In essence, even though a protected trademark is unlawfully incorporated in a website originating in a third state, if the website is "targeted" at consumers in one or more EU Member State, this constitutes infringing use of a trademark within the meaning of Art. 5 of the Trade Mark Directive. Thus, in such circumstances, whether there is a trademark infringement within a particular EU Member State is dependent on whether the counterfeit website is targeted at consumers in that Member State, irrespective of where the website is hosted or the residence of the infringers. Yet, the fact that an infringing website targets the consumers of an EU Member State does not necessary imply that the ISPs operating in that Member State are being used to commit trademark infringement. Nor can it be said that the ISPs play an "essential role" in the infringement. This is because internet users in one Member State may theoretically access any websites hosted by ISPs operating therein, irrespective of whether a website is targeted at that Member State. ISPs do not draw a distinction between websites targeting consumers in the State within which they operate and other websites. In the circumstances, it is difficult to suggest that ISPs in a particular jurisdiction play an "essential role" in (let alone their services being used for) committing trademark infringement even where a counterfeit website hosted overseas targets consumers in that jurisdiction. Thus, the CJEU's guidance could have been sought in relation to the specific question whether the operators of a target counterfeit website make use of the services of the ISPs operating within the jurisdiction in which a blocking injunction is sought – an opportunity that was missed in *Richemont v. Sky*.

Although there are doubts about Arnold J's approach in relying on authorities in the copyright context to support the basis for blocking injunctions in the field of trademark enforcement, this does not mean that the ultimate outcome of the judgement in *Richemont v. Sky*, i.e. the defendant ISPs being required to block access to the target counterfeit websites, is unwarranted. While justifying blocking injunctions in the trademark context is more difficult than in the field of copyright, the wider scope of Sec. 37 of the SC Act provides a better basis for granting a blocking injunction in the UK's context. Thus, a more appropriate approach would have been to utilise the defendant ISPs' knowledge of the infringing nature of the target websites. Once they acquire such knowledge, e.g. through notices or process served on them, it may be persuasively argued that they become subject to a "duty to take proportionate measures to prevent or reduce such infringements even though

[43] *L'Oreal v. eBay*, para. 58.

[44] *L'Oreal v. eBay*, para. 67.

they are not themselves liable for infringement".[45] That duty alone may have been a sound basis for issuing the blocking injunction in the UK. In fact, it seems that this provides a better justification for the existence of the knowledge requirement, even for trademark-related blocking injunctions, than the reasoning offered by Arnold J in his judgement which elucidated a fear that the lack of the knowledge requirement would lead to a general monitoring obligation being imposed on ISPs.[46]

In summary, it may be posited that without a broader domestic legal basis for the grant of a blocking injunction (e.g. the UK's Sec. 37 of the SC Act), it would be difficult to justify an injunction against an ISP in the field of trademarks solely on the basis of Art. 11 of the Enforcement Directive. Thus, in EU Member States where the language of Art. 11 (third sentence) has been strictly transposed into domestic law, the legal basis for blocking injunctions in the field of trademarks would remain problematic for the reasons stated hitherto.

3 A Possible Violation of Natural Justice?

Natural justice (and its terminological variants – due process, procedural fairness or fundamental justice)[47] requires "a decision maker to provide an opportunity to persons affected by a decision to make representation" before a decision is ultimately made.[48] This cardinal principle has been enshrined in legal systems across the globe since time immemorial. More specifically in the IP context, the Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS"), which is one of the several Covered Agreements of the World Trade Organisation ("WTO"), expressly requires all WTO members (including the UK) to ensure that "[d]efendants shall have the right to written notice which is timely and contains sufficient detail, including the basis of the claims".[49] The reference to "defendants" in Art. 42 obviously means the alleged infringers of IP rights. In addition, Art. 42 (fourth sentence) expressly incorporates the right of all parties for a dispute to be heard before a final decision is made.[50] Thus, Art. 42 of TRIPS incorporates the principles of natural justice into the context of IP enforcement. In practical terms, what this means is that in any dispute concerning the infringement of IP rights, it is not only a requirement that the party that is alleged to have infringed a right be notified of the impending proceedings, but also that he be given the opportunity to be heard before a court or other administrative body that goes on to determine the rights and liabilities arising out of a dispute. In fact, although Art. 1(1) of TRIPS permits WTO members to provide more extensive protection than what is required under the agreement, such extra protection cannot be granted in a way that is inconsistent with any other provision of TRIPS, including Art. 42. Thus, it has been observed:

[45] *Richemont v. Sky*, para. 106.

[46] *See supra* note 24 and accompanying text.

[47] Macdonald (1999), p. 573.

[48] Macdonald (1999), p. 574.

[49] TRIPS, Art. 42 (second sentence).

[50] Vander (2009a), p. 705.

> Article 42 prescribes that defendants be accorded due process right in IPR enforcement proceedings. The adoption of more extensive protection that diminishes these due process rights would contravene TRIPS. In this regard, more extensive protection should not include reducing the rights of those asserted to be engaged in infringing acts.[51]

On the other hand, TRIPS has expressly provided for situations where judicial authorities may make *ex parte* orders.[52] This is, however, only possible when a *provisional* order is necessary if a court believes that "any delay is likely to cause irreparable harm to the right holder, or where there is a demonstrable risk of evidence being destroyed".[53] However, TRIPS does not contemplate the granting of an order against an alleged infringer on an *ex parte* basis when that order is anything more than provisional in nature.

These principles of natural justice enshrined in TRIPS extend to the context of blocking injunctions. Where a right-holder seeks to enjoin an ISP compelling it to block access to a website that infringes an IP right, there are, at least, three parties whose rights or interests are at stake. In the EU context, the EU Charter of Fundamental Rights recognises the proprietary rights of IP owners,[54] the interest of the ISPs (to engage in business)[55] and the freedom of speech protecting the authors of content and website operators.[56] By blocking access to a particular website, the interests of the operators of that website will no doubt be affected.[57] In any event, right-holders seeking to block websites do so on the basis that the target websites infringe IP rights. This means that the actual "dispute" is between the right-holders and the target website operators, who are alleged IP infringers. Thus, it may be convincingly argued that before a blocking injunction is granted, a court must hear the persons who operate the target website. Failure to do so would not only breach the principles of natural justice, but also violate Art. 42 of TRIPS.

For these reasons, there is a strong argument in favour of the view that in a typical proceeding where a blocking injunction is sought, a court should afford the right of audience to the operators of the target websites whose rights and interests will be affected in the event that an injunction is granted. Yet, in the UK this is far from the case. Thus, in every single case in which a blocking injunction was granted in the UK, the operators of the target websites – i.e. the actual infringers of IP rights – were neither served with notice, nor heard. The only parties before court were the right-holders and the respective ISPs. This is because, although both the Information Society and Enforcement Directives themselves provide limited guidance as to the parties against whom, and the circumstances in which, a blocking injunction may be obtained, they do not provide any guidance on the procedure that must be followed

[51] UNCTAD-ICTSD (2005), p. 25.

[52] TRIPS, Art. 50(2).

[53] TRIPS, Art. 50(2). *See also* Vander (2009b), p. 743.

[54] EU Charter, Art. 17. IP rights are specifically protected under Art. 17(2).

[55] EU Charter, Art. 16.

[56] EU Charter, Art. 11.

[57] Husovec (2012), p. 123.

in granting such injunctions. In fact, both directives leave it open to the respective EU Member States to determine the conditions and procedures[58] or modalities[59] relating to such injunctions, which has resulted in a divergence in the manner in which the blocking injunction is implemented in various Member States. In the UK, neither Sec. 97 of the CDPA nor any other provision (including Sec. 37 of the SC Act) prescribes the procedure that must be followed in making an application for a blocking injunction. The following observation of Arnold J in *Dramatico v. Sky* clarifies the legal position:

> there is no jurisdictional requirement to join or serve the operators […]. Article 8(3) of the Information Society Directive and section 97A of the [CDPA] confer jurisdiction on the Court to grant injunctions against intermediaries whose services are used by a third party to infringe copyright. Neither Article 8(3) nor section 97A requires joinder or service of the third party.[60]

While this may provide an accurate disposition of the law as it is, by no means is it ideal, especially in view of the following further observation made in *Richemont v. Sky*:

> It is convenient to note at this stage three points about the cases under section 97A. The first is that neither the ISPs nor the rightholders have appealed against any aspect of the orders made in those cases […]. The second is that, since *20C Fox v BT* and *20C Fox v BT (No 2)*, the ISPs have not opposed the making of the orders sought by the rightholders […]. Thirdly, in consequence, most of the orders have been granted after consideration of the applications on paper.[61]

Essentially, what this means is that the court is only possessed of the material submitted by the right-holders, which go uncontested by the ISPs, leaving the interests of the operators of the target websites completely unrepresented. Thus, it may be concluded that the manner in which the blocking injunction is implemented in the UK is, at best, unsatisfactory. Failing to incorporate a procedure to notify, and join in proceedings, target website operators (i.e. the alleged infringers) not only breaches the basic principles of natural justice, but also stands contrary to Art. 42 of TRIPS.

Yet, in the EU context, the absence of the target website operators in proceedings where blocking injunctions are granted is not considered to run counter to principles of natural justice. The following extract from the judgement of the District Court of The Hague in *BREIN v. Ziggo* illustrates this attitude:

> The imposing of the claimed order meets the conditions of due process. After all, the measure is imposed after a prior, fair and impartial procedure, i.e. the present proceedings. Contrary to what [the ISPs] argue, it is not required that

[58] Information Society Directive, Recital 59.

[59] Enforcement Directive, Recital 23.

[60] *Dramatico v. Sky*, para. 10.

[61] *Richemont v. Sky*, para. 4.

> all its subscribers are parties to the proceedings or are heard. [The relevant Dutch law] provides that "the person or persons concerned" must be heard. In a case like the present one, in which an order is claimed against intermediaries, such intermediaries can be considered to be the persons concerned in the sense of this provision. Said intermediaries have been heard. Any different interpretation would render the regulation for orders against intermediaries which the European legislator has implemented with the Enforcement Directive meaningless. It is inherent in such regulation that an order can be imposed upon *inter alia* internet providers to cease their services in proceedings to which the alleged infringer is not, at least not necessarily, a party and so is not heard in it. One of the reasons for implementing such an option is precisely, after all, the situation that the alleged infringer cannot be sued, for instance because his identity is not known.[62]

Of course, this did not mean that courts issued injunctions without going into the merits of a dispute and being convinced of the fact that an underlying infringement was actually taking place. The following UK cases illustrate this fact. Thus, in *Twentieth C. Fox v. BT*, the High Court acknowledged and relied on the findings in *Twentieth C. Fox v. Newzbin*,[63] where the same court found the operators of the Newzbin website to be committing large-scale copyright infringement, although the actual perpetrators were not made party to the subsequent action leading to the blocking injunction. Similarly, in *Dramatico v. Sky* although the right-holders never filed a separate action against the operators of the infringing website in the UK (although both civil and criminal proceedings were filed in other jurisdictions), the High Court went on to first decide whether the website operators and UK internet users were infringing the claimant's copyright.[64] This was the approach adopted in *EMI Records v. Sky*,[65] *Football Association v. Sky*,[66] *Paramount Entertainment v. Sky*,[67] and *Richemont v. Sky*[68]. In other words, only when there is satisfactory evidence of actual infringement taking place will a blocking injunction be issued requiring ISPs to block access to a target website, even though there is no legal requirement that the actual operators of the target website be made party to the action. To be fair, in all of the cases mentioned above, the target websites were patently infringing and thus it would have been disproportionate and futile to expect the right-holders to serve notice and join those persons in the proceedings.

In practical terms, this approach is extremely beneficial to right-holders, especially when the identity of the perpetrators is hidden behind the internet's

[62] *Stichting Bescherming Rechten Entertainment Industrie Neederland (BREIN) v. Ziggo BV and another*, Case 374634/HA ZA 10-3184 (11 January 2012) ("*BREIN v. Ziggo*"). Although the Hague Court of Appeal overturned this judgement on 28 January 2014 (*see infra* note 100), this was on the basis that the injunction was ineffective, and did not raise any issue in relation to due process.

[63] *Twentieth C. Fox v. BT*, paras. 2, 48–55 and 113.

[64] *Dramatico v. Sky*, para. 6.

[65] *EMI Records v. Sky*, paras. 42 and 75.

[66] *Football Association v. Sky*, para. 47.

[67] *Paramount Entertainment v. Sky*, paras. 34–38.

[68] *Richemont v. Sky*, paras. 17–24.

labyrinth of networks. Yet, what must be emphasised is that, in future, there may be instances where the operator of a target website has a plausible defence to a claim of IP infringement. In the circumstances where the court is only privy to the pleadings and documentary evidence submitted on behalf of a right-holder, the court's discretion may become the subject of abuse, especially since the only other party before court (i.e. the ISP) shows no interest in protecting the operators of target websites. Thus, the problem in the manner in which the EU directives are implemented in the UK (and other EU Member States) is that, even in cases where an operator of a target website can be identified and notified of proceedings, the law does not require that to be done. Arguably, such an outcome not only breaches natural justice, but is also contrary to Art. 42 of TRIPS.

4 Inbuilt Safeguards

It is worth noting that blocking injunctions have certain inbuilt safeguards that are aimed at protecting the freedom of expression and preventing abuse on the part of right-holders. To begin with, the very fact that the initial assessment whether a particular website ought to be blocked owing to an underlying infringement is made by a court of law is a significant safeguard against abuse. This is in stark contrast to the N&T approach, where private-sector companies make this judgement, subjecting the regime to immense criticism on the basis that it lacks the necessary transparency, accountability and balance that any dispute resolution system geared against abuse must possess.[69] However, the same criticism does not apply to the "notice and block" regime that the blocking injunction gives rise to, as it is a judicially supervised process.

Blocking injunctions, at least in the UK, have evolved over time, adding to the layers of safeguards. Thus, although in the early stages (e.g. in *Twentieth C. Fox v. BT* and *Dramatico v. Sky*) there were no safeguards in respect of the interests of the operators of the target websites, in *Football Association v. Sky* Arnold J incorporated the following safeguard that was originally introduced by Mann J in an unreported judgement[70] issuing an injunction against the major ISPs blocking access to the "EZTV" website:

> The operator(s) of the Target Website (as defined in the Schedule to this order) and the operators of any other website who claim to be affected by this Order are to have permission to apply to vary or discharge this Order insofar as it affects such an applicant, any such application to be on notice to all the parties and to be supported by materials setting out and justifying the grounds of the application. Any such application shall clearly indicate the status of the applicant and indicate clearly (supported by evidence) that it is the operator of the website which is the subject of the application.[71]

[69] *See e.g.* Adler (2011), Seltzer (2010), Wilson (2009), Urban and Quilter (2006) and Elkin-Koren (2005).

[70] *See* Meale (2013), p. 823.

[71] *Football Association v. Sky*, para. 57.

By the time *Richemont v. Sky* was decided the following layers of safeguards were incorporated which ensures a greater degree of balance and fairness:

1. The possibility for "ISPs to apply to the Court to discharge or vary the orders in the event of any material change of circumstances, including in respect of the costs, consequences for the parties and effectiveness of the blocking measures from time to time".[72]
2. The possibility for the operators of the target websites to apply to the court and have the order varied.[73]
3. The possibility for internet users who are affected by the order to apply to the court and have the order varied. Justice Arnold observed, "future orders should expressly permit affected subscribers to apply to the Court to discharge or vary the orders".[74]
4. In addition, an ISP must provide internet users with accurate and sufficient information pertaining to the blocking of a website. Arnold J was of the view that "the page should not merely state that access to the website has been blocked by court order, but also should identify the party or parties which obtained the order and state that affected users have the right to apply to the Court to discharge or vary the order".[75]
5. The inclusion of a "sunset clause" in all orders, such that the orders will cease to have effect at the end of a defined period unless either the ISPs consent to the orders being continued or the court orders that they should be continued. According to Arnold J, "[t]his will enable the practical operation of the orders to be reviewed in the light of experience".[76]

Although these safeguards play an important role in relation to the human-rights dimension of blocking injunctions, in particular in protecting competition and the freedom of expression on the internet, the second safeguard listed above requires further scrutiny. The opportunity that the operators of target websites have to apply to the court and have the blocking order varied is no doubt a useful safeguard. However, this particular safeguard is diluted in view of the fact that before a blocking injunction is granted it is not a requirement to make the operators of the target websites party to the application. In essence, if a blocking injunction was issued notwithstanding a good defence on the part of the target website operators, by the time they apply to have the order varied by asserting their defence, tremendous damage may have already ensued. The ultimate outcome is that the blocking injunction is not too different from the "act first, ask questions later" type of approach of N&T. Thus, it may be suggested that this safeguard is only meaningful where the operators of a target website cannot be identified at the stage when the court considers the grant of a blocking injunction. In contrast, when in fact the operators of a target website can be identified, their interests are best safeguarded

[72] *Richemont v. Sky*, para. 262.

[73] *Richemont v. Sky*, para. 262.

[74] *Richemont v. Sky*, para. 263.

[75] *Richemont v. Sky*, para. 264.

[76] *Richemont v. Sky*, para. 265.

only if a genuine attempt is made to serve process on them. To that end, the procedure surrounding Sec. 97A of the CDPA, which has also now been adopted as the procedure for injunctions in the trademark context, remains unsatisfactory.[77]

5 Some Practical Considerations

5.1 Circumvention

Since the "knowledge" requirement has been expressly provided for in the copyright context in Sec. 97A of the CDPA, and has now been read into the trademark context in Arnold J's judgement in *Richemont v. Sky*, it might be concluded that the blocking injunction operates as a "notice and block" regime – an injunction only being available against ISPs that have knowledge of the underlying infringement. However, there is an additional reason to regard the blocking injunction as one of "notice and block" – and that concerns the possibility of preventing *future* infringements taking place as a result of circumvention techniques adopted by the operators of infringing target websites.

In order to stress this point, it is necessary to consider the scope and nature of the blocking injunction. For the purposes of this article, it would suffice to refer to the order sought in *Richemont v. Sky*, as that was not only the latest in the series of blocking injunction cases, but also Arnold J considered the plethora of previous decisions in the copyright context – thus resulting in a very comprehensive judgement.

The order sought in *Richemont v. Sky*, in relevant parts, reads as follows:

1. In respect of its residential fixed line broadband customers […], the […] Defendant [i.e. the ISP] shall within 15 working days in relation to the *initial notification (and thereafter, within 10 working days of receiving any subsequent notification)* adopt the following technical means to block or attempt to block access to the Target Websites, their domains and sub-domains and any other IP address or URL notified to the […] Defendant whose sole or predominant purpose is to enable or facilitate access to a Target Website. The technology to be adopted is:

(i) IP blocking in respect of *each and every IP address from which each of the Target Websites operate and which is* […] notified in writing to the […] Defendant by the Applicants or their agents […]

[77] The position in the EU must be contrasted with the regime for blocking injunctions in Singapore and the proposed regime for Australia. Thus, Sec. 193DDB(1) of the Singapore Copyright Act 1987, which was amended in 2014 to introduce a blocking regime, requires that a target website operator be notified of an impending application seeking an injunction. However, the court may only dispense with the notice requirement in circumstances where it is satisfied that despite reasonable efforts the identity of the target website operators cannot be determined. Similarly, in the proposed Australian regime a new Sec. 115A is being introduced into the Copyright Act 1968, which in subsection (4) requires that right-holders make a reasonable attempt to notify the target website operators. Whether such a reasonable effort was made is a factor that a court would take into account in determining whether an injunction ought to be granted (Sec. 115A(5)(h)).

(ii) IP address re-routing in respect of all IP addresses that provide access to *each and every URL available from each of the Target Websites and their domains and sub-domains and which URL is notified in writing* to the […] Defendant by the Claimants or their agents; and

(iii) URL blocking in respect of *each and every URL available from each of the Target Websites and their domains and sub-domains and which is notified in writing* to the […] Defendant by the [Applicants] or their agents.[78]

Thus, it is clear that the identified target websites are blocked using both IP addresses and URLs. Any website that is hosted on a server is assigned a unique address known as an internet protocol address ("IP address") (e.g. 194.33.179.25). Yet, these numbers are difficult to remember and hence are associated with a domain name (e.g. http://www.example.com). The following correlation table provides the domain name and IP address of a single website, namely the website of the UK's Internet Watch Foundation.

Domain name	IP address
www.iwf.org.uk	82.109.189.35

All ISPs use a service known as the Domain Name System ("DNS"), which contains a database of IP addresses and co-related domain names. Each time an internet user wishes to access a particular website (associated with a particular domain name), a request is sent to the relevant ISP's DNS so that the domain name is translated to the IP address to make the connection between the internet user's device (e.g. computer) and the server at which the website is hosted. Thus, a blocking injunction can be implemented using the DNS, "so that when the ISP's DNS server is asked by a customer's computer for the IP address corresponding to the [domain name], the ISP's system either returns no IP address or points the customer to an IP address defined by the ISP that in actuality does not correspond to the [domain name sought to be accessed]".[79] Another approach to achieve a similar result is IP re-routing. Thus, instead of directing the data stream to the IP address of the blocked website, the ISP re-routes the data stream to a pre-defined IP address, thus redirecting users to a different location on the internet, avoiding the blocked website being accessed. Both these techniques allow for blocking using the IP address.[80]

Yet another approach is to use URLs to block access. Thus, ISPs monitor data traffic and block all data associated with a particular blocked URL.[81]

[78] *Richemont v. Sky*, para. 79.

[79] *Richemont v. Sky*, para. 25.

[80] *Richemont v. Sky*, para. 25.

[81] *Richemont v. Sky*, para. 25.

It is in this technological and legal setting that ISPs are obligated to block websites. In order for blocking injunctions to be successful, right-holders must provide ISPs with accurate information containing the IP address and URL of the website that is to be blocked. Thus, once an action seeking an injunction is filed in the High Court, and in the event the injunction is awarded, the ISPs subject to the order must take technical measures to ensure that the target website cannot be accessed by internet users subscribing to the ISPs' services. Doing so would discharge the ISPs' obligations in terms of the injunction.

It is noteworthy that the order cited above refers to both an "initial notification" and a "subsequent notification". Initiating legal proceedings seeking the blocking injunction constitutes the initial notification. A subsequent notification envisages a point in time that is after an ISP's obligatory acts of adopting blocking measures consequent to the award of an injunction.

This possibility a right-holder has in serving an ISP with a subsequent notification is important in view of potential circumvention techniques that may be adopted by those operating the blocked website to overcome the effect of the injunction. 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*".[82] Thus, although the initial blocking of a target website is achieved through the court process, if the perpetrators operating the target website change the target website's IP address (akin to changing the location of an illegal operation) or alter its URL (akin to using a different route to access the website), a subsequent notification providing the new IP address or URL would oblige the ISP to update its system so that the target website remains inaccessible. As such, the blocking injunction – by ensuring that right-holders could notify ISPs of any future changes in the IP addresses and URLs of infringing websites – creates a system that is capable of efficiently combatting circumvention on the part of the operators of the target websites, giving effect to a "notice and block" regime.

Of course, an ISP's blocking measure could easily be circumvented on the part of internet users who subscribe to the services of the ISP.[83] There is, however, very little that can be done to remedy this: "For all blocking methods circumvention by site operators and internet users is technically possible and would be relatively straightforward by determined users. Techniques are available for tackling circumvention, but these are of limited value against sophisticated tools, such as encrypted virtual private networks (VPN)."[84]

Thus, it may be posited that blocking injunctions are more pragmatic in the context of trademark protection than for copyright. As stated earlier in this article – when the correctness of Arnold J's assertion that the services of ISPs are "used" by the operators of the counterfeit websites in order to carry out the underlying infringements was assessed – there is a significant distinction between the way in which copyright and trademark infringements take place on the internet. While in

[82] *Richemont v. Sky*, para. 27.

[83] *Richemont v. Sky*, para. 26.

[84] Ofcom (2010), p. 5.

the copyright context it may easily be concluded that a substantial portion of an ISP's subscribers intentionally access the target websites in order to unlawfully view and download copyright material, a similar assertion cannot be made in the trademark context. As stated before, ISP subscribers are victims rather than co-infringers (with the operators of the target websites). As such, the chances of user-based circumvention are greater in the copyright context than for trademarks – and thus, it is unlikely that an internet user would intentionally undertake circumvention measures to access a blocked counterfeit website. Of course, this may exclude domestic resellers that, for instance, wish to make bulk purchases of counterfeit goods from a blocked website. Nevertheless, the number of such users is negligible in contrast to internet users seeking to gain access to websites committing copyright infringements. Accordingly, blocking injunctions may be more effective in the trademark context.

Despite the possibility of circumvention, on the part of both internet users and operators of infringing websites, Arnold J in *Richemont v. Sky* was of the view that the "notice and block" approach of the blocking injunction was more efficient and effective than N&T.[85] In this regard, Arnold J observed:

> More importantly, Richemont contend that notice and takedown is ineffective because, as soon as an offending website is taken down by one host, the almost invariable response of the operator is to move the website to a different host. *Furthermore, the likelihood is that, sooner or later, the website will be moved to a host, typically based offshore or in a non-Western jurisdiction, which does not respond to notice and takedown requests. Still further, once that happens, the intellectual property owner faces obvious difficulties in jurisdiction and/or enforcement if it attempts to bring proceedings against the host to compel it to take down the website.* I accept that experience in the copyright context bears out Richemont's contentions in this regard. Accordingly, I consider that, while Richemont are open to criticism for not even having attempted to use this measure, it is unlikely that it would be effective to achieve anything other than short-term disruption of the Target Websites.[86]

While the possibility of moving hosts allows the operators of an infringing website to recover from a takedown, it also results in the IP address of the website being altered, thus allowing the circumvention of an ISP's blocking measure. From a technical standpoint, this means that right-holders must take steps to have the content removed at the new host by serving a fresh takedown notice on the new host. Yet, N&T would only become a viable remedy where content-hosts are held accountable for failing to take reasonable steps to avoid or reduce infringements of IP rights. The conditional safe-harbour frameworks envisaged by the US's DMCA (17 USC §512) and the EU's Electronic Commerce Directive (Arts. 12–15) provide the requisite incentives to content-hosts to take appropriate measures to take down infringing content, the failure to do so leading to liability potentially being imputed under the underlying substantive laws. Only a few jurisdictions (e.g. Australia and

[85] *Richemont v. Sky*, paras. 199–204.

[86] *Richemont v. Sky*, para. 201.

Singapore), however, have implemented similar statutory safe harbours consequent to free trade agreements between them and the US. Thus, when infringing content is hosted by content-hosts operating in jurisdictions lacking similar legislative frameworks, the likelihood of those hosts being receptive to a takedown notice is limited. In the circumstances, although a right-holder may resort to serving content-hosts with a takedown notice, the underlying legal framework where the hosts are situated may render the entire process futile. Blocking injunctions, on the other hand, overcome this problem as the blocking takes place not at the source of the infringing website, but rather in the jurisdictions where the ISPs operate. Thus, when circumvention takes place resulting in target websites being hosted in jurisdictions with lax IP laws (making N&T more difficult to achieve), a simple update to the databases of ISPs would enable target websites to be continuously blocked no matter where they are hosted. Thus, it may be submitted that the blocking injunction, at least in the manner in which it is practised in the UK, is capable of effectively tackling circumvention on the part of website operators.

5.2 Multiplicity of Proceedings

Multiplicity of proceedings is a factor that is usually considered under private international law before a court exercises jurisdiction over a given dispute. Usually, where a plaintiff has instituted multiple actions against the same defendants concerning the same dispute, a court may, in applying the principle of *forum non conveniens*, stay proceedings before it on the ground of multiplicity of proceedings.[87]

Since IP rights are often protected globally in multiple jurisdictions, when infringements occur in more than one jurisdiction, right-holders are compelled to file action in every one of those jurisdictions in which their rights are infringed. Yet, in contrast to the conventional understanding of multiplicity of proceedings, in the IP context it is often the case that although the claimants/plaintiffs and the substance of the dispute are the same, the defendants/infringers are not.[88] This applies in relation to blocking injunctions as well.

As was stated before, blocking injunctions target ISPs in order to deal with IP infringements. ISPs operate within the borders of a particular jurisdiction and, therefore, if all ISPs operating within a jurisdiction are targeted, it is possible to completely block access to a target website. This outcome is practically achievable, as in a given jurisdiction there are only a few, or identifiable group of, companies that provide internet access. However, what must be borne in mind is that blocking access to an infringing source in one jurisdiction does not mean that the source cannot be accessed from other jurisdictions. In light of the fact that IP rights are protected globally across multiple jurisdictions, the fact that blocking injunctions are always tied to a particular jurisdiction is problematic.

Thus, if a global level of enforcement is to be achieved, blocking injunctions must be obtained in every single jurisdiction where right-holders have an interest to protect.

[87] *See e.g.* Manolis et al. (2009), pp. 8–9 and Lee (2005), p. 244.

[88] Fawcett and Torremans (2011), p. 289.

The outcome, of course, is a multiplicity of proceedings, although not between the same ISPs. Although the source of infringement is the same, the ISPs operating in each jurisdiction are different. Thus, there is no conceivable mechanism by which a blocking order granted in one jurisdiction could be recognised and enforced in other jurisdictions utilising the standard methods of recognising and enforcing judgements across jurisdictions. Unfortunately, in the EU's context, neither the Information Society Directive nor the Enforcement Directive provides for a means of achieving cross-border enforcement of blocking orders. The problem is more acute since both these directives allow significant discretion as to the conditions and modalities upon which injunctions against internet intermediaries can be obtained. This has led to divergence in respect of both the availability and scope of the type of injunctions capable of being sought in EU Member States.[89] Thus, for instance, apart from the UK, blocking injunctions have been issued against ISPs in countries such as Austria,[90] Belgium,[91] Denmark,[92] France,[93] Ireland,[94] Finland[95] and Italy,[96] whereas blocking injunctions have been refused in Germany,[97] Greece,[98] Spain,[99] Norway[100] and the

[89] For a useful summary of cases where blocking injunctions were sought in EU Member States, *see* Savola (2014), p. 120.

[90] *See UPC Telekabel v. Constantin Film*, Case 4 Ob 71/14 s (24 June 2014). In this case, consequent to the CJEU's ruling, the Austrian Supreme Court allowed a *non-specific* blocking injunction to be issued against an Austrian ISP.

[91] *See Belgian Anti-Piracy Foundation v. Belgacom and Telenet*, Case No. P.13.0550.N/1 (22 October 2013). *See* Vrins and Schneider (2014), p. 306 and Vrins (2014), pp. 873–874 (for more details of this case and an explanation of the Belgian Supreme Court's judgement).

[92] *See Telenor v. IFPI Denmark*, Case No. 153/2009 (27 May 2010). In this case, the Danish Supreme Court allowed the blocking of the infringing http://www.thepiratebay.org website by an ISP on the basis of the DNS blocking technology. For an unofficial translation of the judgement, *see* http://hssph.net/Sonofon_IFPI__DK_SupremeCourt_27May2010_PirateBay.pdf. Accessed 5 July 2015.

[93] *See Association des Producteurs de Cinéma (APC) and others v. Auchan Telecom and others*, Case No 11/60013 (28 November 2013). In this case, the Paris District Court (*Tribunal de Grande Instance*) issued a blocking injunction against a French ISP requiring a website containing infringing copyright material to be blocked using DNS blocking. Interestingly, the court required the cost of implementing the DNS blocking to be borne by the right-holder; *see* Vrins and Schneider (2014), p. 313 (at footnote 566).

[94] *See EMI Records v. UPC*. Here the Irish High Court refused to issue an order requiring an ISP to block access to "The Pirate Bay" website. The Court observed that under current Irish law, there was no basis for the grant of a blocking injunction against an ISP (at para. 122).

[95] Case S 11/3097 (15 June 2012), Case S 12/1825 (8 February 2013) and Case S 12/2223 (11 February 2013). For further information, *see* Savola (2014), p. 124 (and footnote 118).

[96] Case 49437/2009 (23 December 2009).

[97] *See* Case 5U 68/10 (21 November 2013) and Case 6U 192/11 (7 August 2014).

[98] *See e.g.* Case 13478/2014 (22 December 2014). Prior to this case, a blocking injunction was granted in Case 4658/2012. Note that the article written by Savola in 2014 was published prior to the judgement in Case 13478/2014, and hence the table contained therein does not reflect this case.

[99] *See* Savola (2014), p. 125 (and footnote 45).

[100] Although a court in Oslo was expected to issue an order in Autumn 2014 on an application to block The Pirate Bay, at the time of writing it was uncertain whether the order had in fact been issued. *See Russia Today* (2014).

Netherlands.[101] This suggests that there could be problems in utilising the blocking injunction as a means of enforcing IP rights in some EU Member States. Moreover, obtaining blocking injunctions against ISPs in non-EU jurisdictions may be even more problematic, as the laws protecting IP rights may not be as developed as in the EU.

Thus, if the blocking injunction is to develop into a more versatile remedy allowing for enforcement of IP rights on a global basis, a system of recognition and enforcement of judgements (similar to the Hague Convention on Foreign Judgments in Civil and Commercial Matters 1971 or the Brussels Regulations (Recast)[102]) must be adopted in the IP context. For instance, in the EU, where a blocking injunction has already been obtained in one EU Member State, it must be possible for that order to be enforced in other Member States against ISPs operating in those states, since the source of infringement remains the same. This would significantly increase the efficacy of the blocking injunction as a means of enforcing IP.

5.3 Barriers to Legitimate Trade

Both the Information Society Directive[103] and the Enforcement Directive[104] provide that remedies for the enforcement of IP rights must be proportionate. Thus, the principle of proportionality is relevant to the context of the blocking injunction. The fact that such injunctions may be issued only when it is proportionate to do so is a significant safeguard protecting the interests of not just ISPs but also third parties engaging in lawful trade and speech. The principle of proportionality becomes relevant when two or more competing rights conflict and it becomes necessary for courts to reach a balanced outcome. As noted earlier, granting a blocking injunction in favour of protecting IP rights engages two other competing rights: the right to free speech and information and the right to conduct business. These rights, which are protected under the EU Charter, can only be limited "if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others". Accordingly, Arnold J in *Richemont v. Sky* observed:

[101] *Ziggo and another v. Bescherming Rechten Entertainment Industrie Nederland (BREIN)* Case 374634/HA ZA 10-3184 (28 January 2014). The Court of Appeal of The Hague overturned a lower court's decision granting a blocking injunction against two Dutch ISPs. *See* Vrins and Schneider (2014), p. 312 (at footnote 564) for a summary of the case ("The Court of Appeal considered that the blocking order was not effective, since it could be easily circumvented by the 'average' internet user and it appeared from various reports submitted by the online service providers that the order had *indeed* been massively avoided: the Court noted, in this respect, that although the number of visits paid by the subscribers of the service providers concerned on The Pirate Bay had obviously strongly decreased as a result of the implementation of the order, the *total* BitTorrent traffic on the networks of those service providers had remained stable. Therefore, the Court held that the blocking order was in breach of the proportionality principle."). At the time of writing, there is currently an appeal pending in the Dutch Supreme Court seeking a reversal of the Court of Appeal decision.

[102] Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (recast), which came into force on 10 January 2015.

[103] Information Society Directive, Recital 58 and Art. 8(1).

[104] Enforcement Directive, Art. 3(2).

> As for Article 52(1), what this means is that the rights protected by the Charter can only be restricted where this is necessary to protect other rights protected by the Charter. Where two rights, or sets of rights, are in conflict, then the conflict must be resolved by applying the principle of proportionality to each and striking a balance between them. For both reasons, it must be shown that the orders are proportionate.[105]

There is no doubt that if the grant of a blocking injunction amounts to a barrier to lawful trade, including legitimate communications, it is likely to be regarded as disproportionate. In fact, in *Richemont v. Sky*, Arnold J observed that the "impact of [the blocking] measures on lawful users of the internet"[106] is *inter alia* a consideration in determining the matter of proportionality. It was for this reason that he stated that, before the grant of an injunction, the court must be satisfied that "the measures adopted by the ISP [are] strictly targeted so that they do not affect users who are using the ISP's services in order lawfully to access information".[107]

Implementing a blocking injunction to strictly target only an illegal and infringing website is unproblematic where the entire website is designed to promote the infringement of IP rights, as blocking access to the entirety of that website could form a strictly targeted measure that would not interfere with legitimate trade and communications. However, where only part of a website is used to commit infringements, which might be the case with online marketplaces (e.g. eBay) and social networking sites (e.g. Facebook), it would be more difficult to direct a blocking measure to block user access to specific infringing content contained within a website. A case in point is *Ahmet Yildirim v. Turkey*,[108] decided by the European Court of Human Rights ("ECtHR"). This case concerned a measure on the part of the Turkish Telecommunications Directorate ("TTD") to block access to the Google Sites service. The move was motivated as a result of a Turkish court ordering the TTD to block access to a particular site hosted by the Google Sites service. However, the TTD convinced the court to extend the scope of the order on the basis that it lacked the technical capacity to block access to a single site hosted by Google Sites. As such, the ultimate outcome was the blocking of the entire Google Sites service resulting in non-contentious sites also being blocked. The ECtHR ultimately decided that the TTD's action to block access to the entirety of Google Sites was a contravention of Art. 10 of the European Convention on Human Rights that guaranteed freedom of expression. ARTICLE 19, commenting on the judgement observed:

> Blocking access to an entire platform fails to satisfy the requirement that any restriction on the right to free expression online must be strictly limited. Restrictions on freedom of expression must have a clear legal basis, the interference must pursue a legitimate aim, and the restrictions must be

[105] *Richemont v. Sky*, para. 162.

[106] *Richemont v. Sky*, para. 189.

[107] *Richemont v. Sky*, para. 182.

[108] Application No. 3111/10 (18 December 2012). The judgement in English is available at: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-115705. Accessed 5 July 2015.

> necessary and proportionate. Blocking access to an entire platform just because of some illegal content is clearly a disproportionate measure.[109]

The possible impact of blocking injunctions on legitimate internet use was also considered by the CJEU in the series of rulings it made in the context of copyright blocking injunctions. Thus, in *Scarlet Extended v. SABAM*,[110] a Belgian court had ordered an ISP to make "it impossible for its customers to send or receive in any way files containing a musical work in SABAM's repertoire by means of peer-to-peer software, on pain of a periodic penalty".[111] The CJEU was asked whether the imposition of an injunction compelling an ISP to filter all electronic communications passing via its services, in particular those involving the use of peer-to-peer software, applicable indiscriminately to all the ISP's customers and for an unlimited period of time, was consistent with the requirements stemming from the protection of fundamental rights under EU law.[112] In respect of a broad injunction such as this, the CJEU cautioned that the "injunction could potentially undermine freedom of information since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications".[113]

Again in *UPC v. Constantin* the CJEU made it clear that an injunction compelling an ISP to block access to infringing material would only be compliant with EU law if the technical measure does "not unnecessarily deprive internet users of the possibility of lawfully accessing the information available".[114] In the series of cases decided by Arnold J in the UK, culminating in *Richemont v. Sky*, the injunctions related to the blocking of entire websites the sole purpose of which was to infringe IP rights. Thus, we are yet to see how blocking injunctions would operate where only portions of a website contain infringing material. Yet, given the CJEU's guidance on the issue of proportionality, unless infringing material contained amidst other legitimate content could be distinctly isolated and identified for the purposes of blocking, it is likely that a court would find the issuance of a blocking injunction disproportionate, given the danger of suppressing legitimate content. Thus, blocking injunctions may not be an effective remedy in those specific circumstances – the better approach being the use of N&T, which in effect could tackle such delicate scenarios at the very source.

5.4 Cost of Implementation

Lastly, it is worth considering the issue of cost. Interestingly, the Information Society Directive which deals with the enforcement of copyright does not have any specific provision that considers the aspect of cost in the enforcement of copyright.

[109] ARTICLE-19 (2012). *See also* Gurkaynak et al. (2014).

[110] *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL* (Case C-70/10, CJEU) ("*Scarlet Extended v. SABAM*").

[111] *Scarlet Extended v. SABAM*, para. 23.

[112] *Scarlet Extended v. SABAM*, para. 29.

[113] *Scarlet Extended v. SABAM*, para. 52.

[114] *UPC v. Constantin*, para. 63.

However, the matter of cost has seeped into the equation when courts consider the issue of proportionality in the copyright cases that sought a blocking injunction. Thus, for instance in *EMI Records v. Sky*, Arnold J observed that "[s]o far as the cost of complying with a blocking order is concerned, *this is a factor in the proportionality of the order* as between the Claimants and the Defendants".[115] In contrast, Art. 3 of the Enforcement Directive expressly provides that remedies "shall not be unnecessarily complicated or costly".[116] The consideration of cost not only applies to the right-holders, in that seeking relief must not be unnecessarily complicated or costly, but also to the relevant internet intermediaries that are subject to an injunction. This approach was endorsed by the CJEU in *Scarlet Extended v. SABAM* when it observed in the specific circumstances of that case:

> Accordingly, such an injunction would result in a serious infringement of the freedom of the ISP concerned to conduct its business since it would require that ISP to install a complicated, costly, permanent computer system at its own expense, which would also be contrary to the conditions laid down in Article 3(1) of Directive 2004/48, which requires that measures to ensure the respect of intellectual-property rights should not be unnecessarily complicated or costly.[117]

Thus, in *Richemont v. Sky*, Arnold J did consider the issue of cost from the point of view of the ISPs concerned, although this was done as part of the discussion on proportionality.[118] It is clear that the cost of IP enforcement is shared between right-holders and the relevant internet intermediaries. Thus, while right-holders are responsible to bear the cost of taking necessary legal action and also to monitor any circumvention on the part of infringers, the cost of implementing the blocking order and updating the systems to tackle circumvention is borne by the ISPs.[119] Yet, what is important is the consequence of ISPs having to bear the cost of implementing blocking orders.[120] The court observed that while it is true that ISPs already had in place the technological framework to implement blocking orders, such technology often being introduced for other reasons including to deal with the blocking regime of the Internet Watch Foundation,[121] in assessing the ISPs' burden of cost it is necessary to consider "the cumulative cost of implementing all website blocking orders" and not just the "cost of implementing a single order".[122] The defendant ISPs strongly contended that when the cost of implementing Sec. 97A orders under the CDPA were added to the potential cost of implementing trademark-based orders, the costs would undoubtedly skyrocket, especially given the sheer number of counterfeit websites operating at present. Although Arnold J was not persuaded that

[115] *EMI Records v. Sky*, para. 102.

[116] Enforcement Directive, Art. 3 (second sentence).

[117] *Scarlet Extended v. SABAM*, para. 48.

[118] *Richemont v. Sky*, para. 181.

[119] *Richemont v. Sky*, para. 239.

[120] *Richemont v. Sky*, para. 241.

[121] *Richemont v. Sky*, para. 241.

[122] *Richemont v. Sky*, para. 242.

the cost element would prevent an injunction being granted in the specific context of *Richemont v. Sky*, it was clear that the cost factor would play a crucial and important role in future cases, especially in circumstances where the cost really does increase by a large scale.

In addition, it must be pointed out that in all the blocking injunction cases that had come up before the UK courts, *entire* websites were targeted as containing infringing material. We have yet to see a case where only a part, or a very small proportion, of a website is infringing, whereas the remaining parts are perfectly legal. It is unclear as to how this would impact the issue of costs. Presumably, targeting specific parts of a large website requires precision and arguably that may significantly increase the cost of implementing blocking orders in those specific circumstances.

Of course, there are possible avenues to minimise the consequence of costs of implementation. For instance, Arnold J observed: "I do not rule out the possibility of ordering the rightholder to pay some or all of the implementation costs in an appropriate case."[123]

Unless that happens, however, it is likely that eventually the costs involved in implementing blocking orders will have to be passed on to the ultimate ISP users, i.e. consumers. In this regard, Arnold J observed:

> They may either absorb these costs themselves, resulting in slightly lower profit margins, or they may pass these costs on to their subscribers in the form of higher subscription charges. Clearly it is important that none of the ISPs should gain a competitive advantage over the others, but this is ensured by the fact that they are all required to take approximately equivalent measures. Given a level playing field, the ISPs may choose to pass these costs on to their subscribers. The effect of this would be the familiar one of requiring the community as a whole (in this case, the community of broadband users in the UK) to pay the costs of law enforcement action against the minority of people who behave unlawfully or who take advantage of the unlawful behaviour of others (in this case, by accessing infringing websites). This is a solution that has been adopted in many other contexts, most obviously in the funding of police forces through general taxation. It follows that the ISPs would not necessarily be the ones who would ultimately bear these costs. (The same applies to the costs of implementing the IWF blocking regime and parental control systems, of course.)[124]

Yet, the analogy between the tax system, which in part funds the police that enforce the laws of a country in furtherance of achieving public order, and a system by virtue of which the cost of implementing IP rights is passed on to ISP users, requires further scrutiny. The police force exists to maintain public order and therefore expecting a country's citizens to fund its activities is justified, as the ultimate outcome is beneficial to all. In contrast, when only a certain sector of ISP users intentionally access copyright-infringing websites, the same reasoning that

[123] *Richemont v. Sky*, para. 240.

[124] *Richemont v. Sky*, para. 252.

justifies the system of taxation cannot be applied to justify passing the costs of copyright enforcement on to the innocent ISP user-base. While there is no doubt that copyright owners and large industries, including the film and music industries, are hurt by copyright infringements, it is unlikely that the same damage is sustained by innocent ISP users in order to justify them sharing the cost of protecting the interests of copyright owners. In contrast, the analogy drawn by Arnold J arguably better applies to the enforcement of trademark rights through blocking injunctions. Unlike in the copyright context, the availability of websites and online content that infringe trademark rights has the potential of misleading and harming online consumers. In the circumstances, a significant majority of ISP users do not infringe trademark rights, but rather are at risk of being harmed by infringements. Therefore, preventing access to content that infringes trademark rights is in the interest of all internet users. This justifies the cost of enforcing trademark rights through blocking injunctions being passed on to ISP users, just as every citizen must pay taxes which in part fund the police force that in turn protects the citizens.

6 Conclusion

The objective of this article was to critically assess the blocking injunction and its implementation in the UK. A key feature of this remedy is that the internet intermediary that is called upon to block access to infringing websites (or content) does not have to make any determination as to the legality or otherwise of the content sought to be blocked. Unlike the extrajudicial practice of N&T that is currently practised by most US and EU-based internet intermediaries, the blocking injunction is a court-supervised mode of handling infringing content, thereby affording greater transparency, accountability and balance in contrast to the N&T approach. Thus, to a great extent, the criticism levelled against N&T – to the effect that the system is abused by right-holders, leading to the suppression of competing rights and interests (e.g. freedom of expression) – does not, at least on the face of it, apply to the blocking injunction.

Yet, this article noted some problems with this form of injunctive relief. First, having considered the legal basis for the injunction, it was argued that the requirement that an intermediary's services must have been *used* to commit an IP infringement creates problems in the field of trademark enforcement. Unlike in the copyright context, where an ISP's subscribers are often co-infringers with the operators of an infringing website, the same cannot be said when an internet user accesses a counterfeit website and makes a purchase of an item he/she believes to be authentic. Internet users are victims, rather than infringers. Nor could it be argued that counterfeit website operators (often operating from overseas) have used the services of domestic ISPs to commit infringements. Thus, the legal basis for the blocking injunction in the trademark context remains suspect.

Secondly, it was noted that in the UK (as in the case of the EU) there is no legal requirement that the operators of target websites be notified of, or joined in, proceedings consequent to which their websites are likely to be blocked. This article argued that this situation is contrary to the principles of natural justice, and in

particular to Art. 42 of TRIPS, which requires that all parties whose rights are likely to be affected must be afforded an opportunity to present their case before a decision is made. Although a safeguard does exist allowing target website operators to apply to court to have a blocking order varied or vacated, that safeguard is diluted in the absence of a notice requirement. Thus, by the time a target website operator becomes aware of a blocking order, significant damage may have already occurred.

Lastly, the article focused on four practical aspects: i.e. circumvention, multiplicity of proceedings, barriers to legitimate trade and costs of implementation. With respect to circumvention, it was noted that the approach in the UK, which allows right-holders to notify ISPs of changes in target websites (resulting in circumvention) so that ISPs' databases could be updated, is a significant judicial innovation aimed at tackling circumvention. Yet, there is little that can be done (in terms of the current state of technology) to prevent user-based circumvention. However, unlike in the field of copyright enforcement, user-based circumvention is negligible in the context of trademark enforcement. Thus, blocking injunctions are more efficient for protecting trademark rights.

With respect to multiplicity of proceedings, it was noted that the fact that blocking injunctions are tied to a particular jurisdiction, although IP rights are often required to be protected in multiple jurisdictions, inevitably would lead to a multiplicity of proceedings. Existing frameworks for the mutual recognition and enforcement of judgements cannot be applied to this context, as even though the source of infringement is the same, the ISPs against whom the blocking injunctions are directed vary from country to country. Thus, unless a global (or EU-wide) framework is formulated where blocking orders could be recognised and enforced in multiple jurisdictions, multiplicity of proceedings may remain an issue, especially in view of the universal reach of most websites and online content; hence, the need for a global level of protection.

This article then considered the issue of proportionality. Blocking measures must not hinder legitimate trade. If they do, they would be deemed disproportionate. In the UK, blocking orders have been used to block entire websites that were infringing IP rights. Yet, in future, if there is a need to block only a very specific part of a website, where the remaining parts are legitimate, unless blocking orders can be targeted accurately, without significantly adding to the cost factor, this remedy may be rendered unsuitable.

Finally, the article evaluated the cost of implementing blocking orders. While it is clear that ultimately the cost of implementation is likely to be passed on to the internet users, the analogy that Arnold J drew between an increase in subscription fees and the tax system is somewhat questionable. While it is true that taxes fund the police force to maintain public order, that justification is less applicable to the copyright context. Unlike in the case of a safe and orderly society that benefits everyone living in it, protecting copyright directly benefits right-holders, although only indirectly benefits society at large. Yet, the tax analogy is more suitable to the context of trademark protection, as protecting trademarks has the direct consequence of consumer protection. Thus, an increased subscription fee that goes on to fund blocking orders on the part of ISPs has a better justification in the field of trademarks.

References

Adler J (2011) The public's burden in a digital age: pressures on intermediaries and the privatization of internet censorship. J L Pol'y 20:231

ARTICLE-19 (2012) Turkey: Landmark European court decision finds blanket Google ban was a violation of freedom of expression. http://www.article19.org/resources.php/resource/3567/en/turkey:-landmark-european-court-decision-finds-blanket-google-ban-was-a-violation-of-freedom-of-expression. Accessed 5 July 2015

Elkin-Koren N (2005) Making technology visible: liability of internet service providers for peer-to-peer traffic. New York Univ J Legis Pub Poly 9:15

Fawcett JJ, Torremans P (2011) Intellectual property and private international law, 2nd edn. Oxford University Press, Oxford

Gurkaynak G, Yilmaz I, Durlu D (2014) Exploring new frontiers in the interface between free speech and access bans: the European Court of Human Rights Case of *Ahmet Yıldırım v. Turkey*. EJLT 5. http://ejlt.org/article/view/282/425#_ftnref50. Accessed 5 July 2015

Headdon T (2012) Beyond liability: on the availability and scope of injunctions against online intermediaries after L'Oreal v Ebay. EIPR 34:137

Husovec M (2012) Injunctions against innocent third parties: the case of website blocking. JIPITEC 4:116

Husovec M, Peguera M (2015) Much ado about little—privately litigated internet disconnection injunctions. IIC 46:10

Lee J (2005) Private international law in the Singaporean courts. SYBIL 9:243

Macdonald RA (1999) Natural justice. In: Gray CB (ed) The philosophy of law: an encyclopedia. Routledge, London, pp 573–575

Manolis FM, Vermette NJ, Hungerford RF (2009) The doctrine of forum non conveniens: Canada and the United States compared. FDCC Quarterly 60:3

Meale D (2013) Premier League 1, Internet pirates 0: sports streaming website the latest to be blocked. J Intell Prop. L Pract 8:821

Ofcom (2010) "Site blocking" to reduce online copyright infringement. http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf. Accessed: 5 July 2015

Russia Today (2014) Anti-piracy group to fight Pirate Bay in Norway court. http://on.rt.com/oog6y1. Accessed 5 July 2015

Savola P (2014) Proportionality of website blocking: internet connectivity providers as copyright enforcers. JIPITEC 5:116

Seltzer W (2010) Free speech unmoored in copyright's safe harbor: chilling effects of the DMCA on the first amendment. Harv J L Tech 24:171

UNCTAD-ICTSD (2005) Resource book on TRIPS and development. Cambridge University Press, Cambridge

Urban JM, Quilter L (2006) Efficient process or "chilling effects"? Takedown notices under section 512 of the Digital Millennium Copyright Act. Santa Clara Comput High Tech L J 22:621

Vander S (2009a) Article 42: fair and equitable procedures. In: Stoll P, Busche J, Arend K (eds) WTO—Trade-Related Aspects of Intellectual Property Rights. Koninklijke Brill NV, The Netherlands, pp 702–707

Vander S (2009b) Article 50: Administrative procedures. In: Stoll P, Busche J, Arend K (eds) WTO—Trade-Related Aspects of Intellectual Property Rights. Koninklijke Brill NV, The Netherlands, pp 738–750

Vrins O (2014) The EU policies and actions in the fight against piracy. In: Stamatoudi I, Torremans P (eds) EU copyright law: a commentary. Edward Elgar, Cheltenham, pp 799–945

Vrins O, Schneider M (2014) Cross-border enforcement of intellectual property: The European Union. In: Torremans P (ed) Research handbook on cross-border enforcement of intellectual property. Edward Elgar, Cheltenham, pp 166–328

Wilson B (2009) Notice, takedown, and the good faith standard: How to protect internet users from bad-faith removal of web content. St Louis U Pub L Rev 29:613