Looking above and beyond the blunt expectation: specified request as the recommended approach to intermediary liability in cyberspace

Krzysztof Garstka [1]

Cite as Garstka K., "Looking above and beyond the blunt expectation: specified request as the recommended approach to intermediary liability in cyberspace", in European Journal of Law and Technology, Vol 7, No 3, 2016.

ABSTRACT

Following the publication of the Digital Single Market agenda, it became clear that establishing the place of online intermediaries in the regulatory framework for combating illicit content on the Internet remains one of the key challenges for European regulators. This article looks at the landscape of corresponding enforcement strategies within the European Union and unravels two competing conceptual approaches in relation to the role of online intermediaries. The first one, characterised as "blunt expectation" is based on exploiting the intermediaries' fear of liability for the actions of their users, in order to have the former take unspecified actions towards the infringements, or refrain from conducting their services altogether. The second approach, labelled as "specified request", is based on requiring the intermediaries to implement specific procedures or elements of infrastructure, with the liability arising not from the infringements of the users, but from the lack of compliance with the stipulated requirements. After comparing the merits and demerits of both approaches, the author puts forward an argument in support of greater reliance on the specified request approach, and elucidates the challenging, yet worthwhile path to its implementation within the EU.

Keywords: Intermediary liability; content liability; EU law; information technology law; copyright; trademarks; privacy; defamation; E-Commerce Directive; human rights

1. INTRODUCTION

On the 24th of September 2015, the EU Commission launched a public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy.[2] The consultation document contains a section on "(t)ackling illegal content online and the liability of online intermediaries". [3] It is clear that determining the duties of the Information Society Service Providers [4] (hereafter referred to as the ISSPs) in relation to various types of infringing content is equally vital and challenging: a notion often underlined by different commentators, in different tones. The Digital Music Report prepared by the International Federation of the Phonographic Industry (hereafter referred to as the IFPI) stated that such intermediaries are "uniquely situated" [5] to help in tackling the problem of pirated copyrighted works - and, one could propose, other types of infringing content as well. Edwards probably put it more accurately, when she wrote that the Internet Service Providers (and, it could be added, many other online intermediaries) "hold an unfortunate piggy-in-the-middle position".[6]

In the last two decades, two primary conceptual approaches aimed at regulating the role of intermediaries in the enforcement process have emerged. The first approach can be referred to as that of "blunt expectation". It is based on escalating the intermediaries' fear of liability for the actions of their users, in order to have the former take unspecified actions towards the infringements, or refrain from conducting their services altogether; both outcomes are supposed to result in the cessation of infringing activities. In its purest form, this doctrine places a threat of punishment without offering any guidance whatsoever on how to avoid it. In order to shed more light on the core of blunt expectation, a comparison might be made between the information passing through the ISSP's service, and dangerous animals. According to section 2(1) of the UK Animals Act 1971, the keepers of animals belonging to dangerous species are to be strictly liable for any damage caused by such animals; as Giliker writes, liability in such situations arises "regardless of fault, and irrespective of any awareness of the animal's dangerous propensities". [7] Furthermore, the Act does not specify the measures which ought to be taken by the keepers, what kind of a cage they should be keeping the tigers in, whether they should keep an eye on the crocodiles during the night etc. By opening their services to online traffic, the ISSPs might be regarded as keepers of (potentially) dangerous information, who should be solely responsible for choosing and implementing the steps aimed at ensuring that such information is not roaming the cyberspace and causing harm to the rightsholders. Such a view of intermediary liability strongly reflects the core of the blunt expectation doctrine.

On the other side of the conceptual line lies the stance labelled in this article as the "specified request" approach: it differs from blunt expectation in two key, intertwined aspects. Firstly, instead of crudely expecting the ISSPs to deal with the infringements on their own and burdening them with the consequent effect-based demands, this approach invites the legal systems to require ISSPs to implement specific procedures or elements of infrastructure, indicated with as much precision as possible. Secondly, due to its focus on delineating the ISSPs' obligations, this approach strives to achieve its aim by favouring the doctrine based on liability arising not from the infringements of the users, but from the lack of compliance with the prescribed enforcement procedures and requirements. In its purest form, specified request lays out such procedures and requirements in so much detail, that there are no interpretative challenges left for the intermediary, who simply ought to follow the outlined obligations.

The argument furthered in this paper is that - with adequate space left for the particularities of different online services and content types - the specified request approach offers a significantly better policy direction, and that it should be implemented at EU level through a major regulatory reform, giving it more prominence in the enforcement landscape than it is given right now. It is submitted that this approach is better at the general, conceptual level, and also that the introduction of well-tailored specific requirements could improve on the shortcomings of the current online content regulation policy, permeated by the blunt expectation approach.

In order to support the submissions of the preceding paragraph, the article adopts the following structure. Section two elaborates on the description of each of the two approaches by demonstrating their regulatory presence with reference to multiple types of infringing content and corresponding regulatory measures. It has to be noted that the regulatory responses are lying on different points between the two extremes of the discussed doctrines. The third section considers the merits of both approaches, presenting a case in favour of the specified request approach. Finally, the concluding section proposes a path through which the specified request approach could be implemented within the legal framework of the EU, and sets out the key resulting questions and concerns which would need to be answered in that eventuality.

2. THE TWO APPROACHES TO INTERMEDIARY LIABILITY

2.1. THE BLUNT EXPECTATION APPROACH

A good example that demonstrates the blunt expectation approach at work is placing the threat of civil and criminal liability on online intermediaries for the actions of users. Within the EU, it is possible to find dozens of legal measures leading to this outcome; for the purpose of this paper, a selection of such liability doctrines was chosen.

2.1.1. BLUNT EXPECTATION AND THE CIVIL LIABILITY OF INTERMEDIARIES

Two modes of civil liability were chosen as examples for this section; joint tort liability and publisher's liability. In English law, joint tort liability arises whenever two or more parties become liable for the same tortious loss suffered by the claimant; with the loss having been caused by - for example - the infringement of claimant's copyright, trademark, privacy or reputation. However, it is crucial for those parties to have acted in a certain form of agreement, as demonstrated by the words of Lord Templeman in the case of *CBS v Amstrad*:[8] "joint infringers are two or more persons who act in concert with one another pursuant to a common design in the infringement". [9]

The use of joint tort liability against online intermediaries can be demonstrated by reference to two UK cases; the first one being *L'Oréal v eBay*.[10] As a matter of introduction; over the years, sellers of counterfeit goods started using eBay, especially those bearing the trademarks of companies producing luxury goods. One such company, L'Oréal, sued eBay for facilitating the trade in goods infringing their trademark. Initially, Arnold J identified the factors which could indicate that the operators of eBay were jointly liable for trademark infringements of the platform's users, stating that the former:

> "(…) do *facilitate* the infringement of third parties' trademarks, including L'Oréal's Trade Marks, by sellers; they do *know* that such infringements have occurred and are

> likely to continue to occur; and they *profit* from such infringements except where the rights owner makes a VeRO complaint [11] in sufficient time". [12]

However, the judge stated immediately after that "these factors are not enough to make eBay Europe liable as joint tortfeasors (…)" for "it cannot be said that the facility is one which inherently leads to infringement. It is capable of being used by sellers in a manner which does not infringe third party trademarks". [13]

This decision can be seen as complemented by the *Fox v Newzbin*[14] case. Here, the operators of a Usenet indexing website (which was found to have been used for the illegal exchange of copyrighted movies) were sued by Twentieth Century Fox and found liable for the infringing activities of their users. While the judge referred to *L'Oréal v eBay*, he found the facts of the Usenet indexing service's case to be leading to a different outcome. Newzbin was found to have acted in common design with the infringers (the premium members, specifically), and hence, to be jointly liable with them. Kitchin J declared that:

> "(…) the defendant well *knows* that it is making available to its premium members infringing copies of films, including the films of the claimants. In summary, the defendant operates a site which is *designed and intended to* make infringing copies of films readily available to its premium members; the site is structured in such a way as to promote such infringement by guiding the premium members to infringing copies of their choice and then providing them with the means to download those infringing copies by using the NZB facility". [15]

If we take away any evidence showing the existence of a common design (for e.g., internal e-mails), it is quite difficult to see a clear line drawn by those two cases between an online service which was designed and intended to be used as a means for spreading infringing content, and a service which attracted a significant amount of infringing activity without such tortious intent. It seems plausible to state that the actual amount of infringing and non-infringing activity on the service, independent of the operators' intentions, played a considerable, indirect role in the different treatment of both services.

What is, however, shared by those two cases is that they remain, in large part, a representation of the blunt expectation approach and its two key components. Firstly, despite a valuable set of guidelines proposed by Arnold J in *L'Oréal*, [16] and a broad preventive filtering injunction granted in *Fox v Newzbin* [17] (both of which constitute steps towards the specified request) neither of the two decisions specifies what is it that the content-hosting or content-indexing ISSPs should do in order to avoid joint tort liability, or what procedures or solutions they should endorse. Furthermore, both cases oblige the intermediaries to tackle the infringements or face liability for the actions of the primary infringers.

Another mode of liability supporting this regulatory approach is publisher's liability. It is a very good example for showing how a seemingly clear word from the everyday language might gain a whole new dimension of complexity upon being incorporated into the legal language, especially when such language is employed to tackle the legal challenges of cyberspace. It also demonstrates how a legal concept might change in the online setting, as noted by Reed in the context of publisher's liability in defamation cases. [18] To demonstrate publisher's liability in practice, the following paragraphs will discuss two such cases from the UK, together with a French copyright decision.

The first case to be presented in this section is *Godfrey v Demon Internet*.[19] The defendant ISP was held liable for the defamatory posts published on a Usenet newsgroup hosted by the ISP. It was established that as soon as an online service provider becomes aware (i.e. acquires actual knowledge) of the defamatory use of its service, it becomes liable in common law as a publisher of the defamatory information. Then, it has to remove the infringing content expeditiously in order to prevent further dissemination of the defamatory material - or become liable in damages to the claimant. [20] While on its own, the requirement of expeditious removal is tied to the notion of specified request, *Godfrey* can be seen as representing the blunt expectation approach not only due to the strong focus on the threat of liability for users' actions, but also due to the variety of questions it leaves unanswered (discussed in section 2.2.1 below).

The second case did not end with a finding of publisher's liability, but it can be seen as a sign of this approach being suggested, at least towards certain categories of intermediaries. In *Bunt v Tilley*,[21] three different ISPs (AOL, Tiscali and BT) found themselves targeted by a claim based on publisher's liability for defamatory statements. The difference from *Godfrey* is that they were not hosting a newsgroup where defamatory posts could appear - they were sued for the mere provision of the internet connection which was used by their subscribers to post defamatory messages on third party websites. However, the court found that the three ISPs cannot be regarded as publishers of the defamatory statements - instead, they should be seen as passive facilitators, lying outside of the scope of publisher's liability. The key factor which might bring an online intermediary within the role of a publisher was characterised by Eady J as "knowing involvement in the process of publication of the relevant words". [22] Such conduct would be seen as moving the service provider outside of the "passive, instrumental role in the process" [23] - and this was not found to be the case for AOL, Tiscali and BT. While the claim failed, the proceedings stand as a testimony to the rightsholders' efforts aimed at making the purer versions of the blunt expectation approach dominant in the debate on intermediary liability. Hence, even if liability was not found in *Bunt v Tilley*, it is worth discussing this case in the current section of the paper.

The operators of the music streaming website Myspace were less fortunate than the ISPs in *Bunt v Tilley*. While the French Tribunal of Grand Instance found this portal to be a hosting provider, shielded from liability by virtue of ArticleArticle 14 of the E-Commerce Directive,[24] it was also found to be a publisher of content, and on this basis, the French TGI stated that the operators of Myspace can be liable for the copyright-infringing conduct of their users.[25] The operators were placed within the role of a publisher, because they went beyond mere storage and communication of content, by organising and presenting the content in a specific manner, as well attaching advertisements to the hosted content. [26] The notion of profit tied to the transfer of copyright-infringing information, combined with an increased amount of interaction with the hosted content (found in, for e.g., editing activities), were sufficient to enable the blunt expectation approach in the form of publisher's liability.

2.1.2. BLUNT EXPECTATION AND THE CRIMINAL LIABILITY OF INTERMEDIARIES

The criminal liability aspect of the blunt expectation approach is demonstrated by reference to two UK offences; the conspiracy to defraud and the copyright offence of communicating the work to the public in the course of a business.

Starting with the former; the key definition of conspiracy to defraud was given in the case of *Scott v Commissioner of Police of the Metropolis*,[27] where Viscount Dilhorne described it as

an "agreement by two or more by dishonesty to deprive a person of something which is his or to which he is or would be or might be entitled and an agreement by two or more by dishonesty to injure some proprietary right of his". [28] The highest available penalty for this offence is ten years of imprisonment and/or an unlimited fine.

The case of *R v Allan Ellis*[29] can serve us here as the first example of the use of conspiracy to defraud against a relevant online intermediary. The defendant in those proceedings operated a BitTorrent-oriented music sharing website known as Oink's Pink Palace. In 2007, using the charges of conspiracy to defraud, the British police arrested the website's operators and Oink's servers (placed in the Netherlands) were seized. The Middlesborough Crown Court found the defendant operators to have acted dishonestly and refused to apply the E-Commerce Directive's safe harbour; however, the jury acquitted the defendants. [30] Additionally, this case stands (among others) as a testimony of the reach of criminal liability of intermediaries: this type of liability enables the use of cross-border enforcement measures (such as the seizure of servers).

The second offence is set out in s. 107(2A) of the Copyright, Designs and Patents Act 1988 c. 48 (CDPA 1988). It criminalises infringing the copyright in a work by communicating the work to the public in the course of a business, or (if not in the course of a business) to such an extent that the copyright owner is prejudicially affected.[31] Those found guilty are liable to be imprisoned for up to three months and/or fined with the amount not exceeding 50,000 GBP (summary conviction), or imprisoned for up to two years and/or fined with an unlimited sum of money (conviction on indictment). [32]

At the time of writing, s. 107(2A) of the CDPA 1988 has not produced any noticeable legal decisions in terms of online intermediary liability. However, in June 2013, the police began targeting various file-sharing websites with letters with the wording: "We have grounds to suspect that as owners and/or operators of the XXXXX website, you are committing the offence of communication to the public under s.107 (2A) of the Copyright, Designs & Patents Act 1988 ("CDPA")". [33]

Neither the described application of conspiracy to defraud, nor the British police's letters based on section 107(2A) set out the actions to be taken by the ISSPs wishing to avoid criminal liability for their users' infringements. Both these enforcement strategies are based on the threat of punishment, in the form of fines, imprisonment and seizure of property. As such, those initiatives fall strongly within the blunt expectation category, in an even stronger manner than the civil liability examples, due to the arguably more severe punishment and the stigma awaiting the intermediaries who fail to "handle" the infringements occurring on their services.

Should a regulator wish to further follow the blunt expectation approach, the path they ought to take is twofold. On the one hand, he can change the law to create new modes of liability or enhance the penalties attributed to ones which already exist. On the other, he can ramp up the enforcement efforts based on the law as it stands; for example, through further initiatives akin to that of the police noted above.

2.2. THE SPECIFIED REQUEST APPROACH

In contrast to the blunt expectation variant, the degree of reliance on the specified request approach is less apparent. Throughout the EU, the ISSPs are still mostly subjected to some form of the former; nevertheless, there are some signs of the latter scheme being endorsed.

The ones to be discussed in this section are - the notice and takedown-prompting Article 14 of the E-Commerce Directive 2000/31; the "Newzbin 2" blocking injunctions from the UK; the filtering requests made in the CJEU cases of *Scarlet Extended*[34] and *Netlog*,[35] as well as in the German BGH case of *GEMA v Rapidshare;*[36] the website blacklist made for online advertisers by the UK's Police Intellectual Property Crime Unit (PIPCU); and finally, the Memorandum of Understanding on Counterfeit Products, signed under the auspices of the EU Commission. This is admittedly a fairly lengthy list, due to the fact that each of those regulatory initiatives belongs to the specified request doctrine in a different manner.

2.2.1. THE SPECIFIED REQUEST AND NOTICE AND TAKEDOWN

Article 14 of the E-Commerce Directive protects the providers of hosting services from liability for illicit content, provided that they do not have actual or constructive knowledge of its presence. Should they obtain this knowledge, they have to act expeditiously to remove access to the said content, in order to benefit from Article 14the protection under Article 14. This provision, inspired by the US' DMCA 1998 [37] and resembling the logic of *Godfrey*, can be indicated as the main propeller of the notice and takedown schemes within the EU. The core logic of such schemes falls strongly within the specified request, with rightsholders and intermediaries working together to tackle infringing content on the latter's services.

However, Article 14 left many questions and over the years, the Member States' courts struggled to provide coherent, precise answers to them. Such questions include: what is "expeditious removal"? Can a notice be sent against an online account? In what manner should the factors nullifying the infringing character of content be considered by the intermediaries, as well as the rightsholders themselves? The specified request nature of notice and takedown schemes would be reinforced if those questions found precise, harmonised answers, and if the threat of liability for users' actions was to be replaced by a more independent obligation to operate the enforcement procedure discussed here. Section 4 of this paper proposes the foundation of a system which could govern such obligations.

2.2.2. THE SPECIFIED REQUEST AND NEWZBIN 2 INJUNCTIONS

The term "Newzbin 2 injunctions" refers to a continuously growing streak of website-blocking orders awarded in the UK against websites for IP-infringing activities. The injunctions derive their name from the fact that the case in which the first one was given was focused on the reactivated version of the Newzbin website (Newzbin2), following the initial proceedings. [38] Upon noticing the reinstatement of the website, Fox decided to change the approach and, through the case of *Twentieth Century Fox Film Corp v British Telecommunications Plc*[39] (*Fox v BT*), successfully applied for a blocking injunction against Newzbin2, based on section 97A of the CDPA 1988. This provision of the UK law, giving effect to Article 8(3) of the Information Society Directive,[40] states that "the High Court (in Scotland, the Court of Session) shall have power to grant an injunction against a service provider, where that service provider has actual knowledge of another person using their service to infringe copyright".

Here, the requested injunction was aimed at forcing BT (the largest ISP in UK) to prevent its subscribers from accessing the Newzbin2 website. In the following years, similar blocking orders were granted against multiple online intermediaries, through decisions such as *Dramatico Entertainment v British Sky Broadcasting (No. 2)*, [41] *EMI Records Ltd v British Sky Broadcasting Ltd*, [42] *Football Association Premier League Ltd v British Sky Broadcasting Ltd & Others* [43] and *Paramount Home Entertainment International Ltd v British Sky Broadcasting Ltd*. [44] Additionally, it is worth mentioning that with the decision in *Cartier International AG*

v British Sky Broadcasting Ltd (2014), [45] a number of websites advertising and selling counterfeit goods were blocked in a similar way on the basis of the generic s. 37 of the Senior Courts Act 1981, [46] thus expanding the website blocking injunctions to the realm of trademarks.

Within those decisions, there is a clearly specified obligation - to block access to the indicated website(s). Furthermore, given that a specific technology (the Cleanfeed system [47]) was indicated in the order awarded in *Fox v BT*, [48] the process of obtaining such orders became streamlined (as Mac Sithigh noted [49]). There is also a distinct lack of attempts to make the defendant ISPs liable in damages for the infringements occurring on the blocked services, it seems that this line of online enforcement is firmly drawn towards the specified request approach. [50]

2.2.3. THE SPECIFIED REQUEST AND PREVENTIVE CONTENT FILTERING

The next trace of this doctrine comes from the CJEU cases of *Scarlet Extended* and *Netlog*. While *Scarlet* dealt with copyright infringements occurring via P2P networks, and *Netlog* with those appearing on a social networking platform, the injunctions sought by SABAM, the claimant, were similar. In *Scarlet*, the ISP challenged a Belgian court order which obliged it to "bring to an end the copyright infringements established in the judgment of 26 November 2004 by making 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". [51] In *Netlog*, the social network also challenged an order which requested the termination of infringements to claimant's copyright, occurring on the former's platform. [52] As the CJEU phrased it, both orders asked for filtering of information covering all services' users indiscriminately, as a preventative measure, exclusively at the hosting providers' expense and for an unlimited period. [53] Both were dismissed as incompatible with the EU law, primarily due to the threats they posed for the freedom of expression, the right to privacy, and the freedom to conduct a business. [54]

Furthermore, it is also worth mentioning the BGH's decision in the German case of *GEMA v Rapidshare*. While *Scarlet* and *Netlog* entailed filtering on the defendant's own service, the injunction granted in *GEMA v Rapidshare* obliged the operators of this file-hosting website to "find out through general search engines like Google, Facebook, or Twitter using applicably formulated search enquiries and, where appropriate, also so-called web crawlers, whether references to further infringing links to Defendant's service can be found (…)". [55]

Orders such as those in *Scarlet* and *Netlog* fall into a strange place between the specified request and blunt expectation approaches. On the one hand, one would be tempted to characterise them as an aspect of the former, as the order specifies what it is that an ISSP should do, contrary to for e.g., a claim in damages based on a variant of civil liability. However, on the other hand, those orders were extremely broad in asking the intermediaries to "prevent infringements"- what draws them towards the blunt expectation approach. The *GEMA* case is different; the request is much more specific. However, it is difficult not to notice that BGH's order is potentially an extremely burdensome one, maybe even impossible to comply with. It is difficult to see it as a positive outcome of the specified request approach, and together with the two CJEU decisions, the decision in *GEMA* seems to indicate that the judges might not be the best suited party to create the landscape of specific procedures which the intermediaries ought to implement on their services.

2.2.4. THE SPECIFIED REQUEST AND THE PIPCU BLACKLIST

The PIPCU's blacklist represents the so-called "follow the money" approach to tackling online infringements of IP rights, supported (among others) by entities such as Google [56] or the European Commission. [57] The blacklist is a part of an initiative dubbed "Operation Creative", and consists of a list of websites deemed to be "copyright infringing sites, identified by the creative industries and evidenced and verified by the City of London Police unit": providers of online advertising services are encouraged to cease the provision of their services to such websites. [58] The encouragement factor might be enhanced by the fact that the major bodies representing the advertising industry in the UK are partners to Operation Creative.

The request conveyed by the PIPCU is a very narrow and specific one - to cease the provision of services to a detailed list of websites. As such, it falls strongly into the specified request category. Of course, this list is not legally binding (and even if it was, it would not cancel out the possibility of acquiring secondary liability), and there are providers of advertising services who are less likely to implement the blacklist (for e.g., "rogue" services based outside of the UK); nonetheless, it can be identified as one of the more prominent shifts towards the specified request approach (especially due to the fact that on its own, this initiative does not impose liability for actions of the advertising service's users).

2.2.5. THE SPECIFIED REQUEST AND THE MEMORANDUM OF UNDERSTANDING ON COUNTERFEIT TRADE

The Memorandum of Understanding on the sale of counterfeit goods on the Internet [59] is a voluntary agreement signed under the auspices of the EU Commission by multiple stakeholders, most importantly the "right owners" and "internet platforms". Both categories of signatories pledge to follow a code of practice tied to tackling the infringement of IP rights occurring through the online trade in counterfeit goods. The operators of services agreed, among others, that notice should be sent to the account of a user who uploaded the content, [60] that they ought to facilitate the users' ability to identify and report rogue sellers and their offers, [61] and that they should undertake their "best efforts" aimed at preventing the re-registration of repeat offenders whose accounts were shut down. [62] Even preventive filtering, despite being a major point of contention in the enforcement debate received a mention,- the Internet platforms pledged to "take appropriate, commercially reasonable and technically feasible measures, taking into consideration their respective business models, to identify and/or prevent proactively the sale of Counterfeit Goods(...)". [63]

In return, and this is where the specified request approach strongly marks its presence, the rightsholders stated (jointly with the platform operators) that "(i)n order to facilitate an atmosphere of good faith, in which the signatories are willing to cooperate and assist each other in the fight against the sale of Counterfeit Goods over the Internet, the signatories *agree not to initiate any new litigation* against each other, concerning matters covered by this MoU". [64] Despite the lack of binding legal power and a limited content focus, the Memorandum is probably the strongest representation of the specified request approach within the European enforcement landscape, and a potential sign on the road leading towards a fuller realisation of this strategy. This position can be seen as reinforced by the *IP Enforcement 2020* report of the UKIPO, which indicates relying on the Codes of Practice for intermediaries as one of the main directions for online enforcement.[65]

3. WHY IS THE SPECIFIED REQUEST APPROACH GENERALLY BETTER?

While the exact details of requirements which could be applied to different intermediaries (as well as to different content types and forms) can - and should be - the subject of a further, robust debate, this article can already propose that the specified request approach is better at the general, conceptual level, and that an adequately shaped set of specific requirements could improve on the shortcomings of the online content regulation policy influenced by the blunt expectation approach. It is not suggested that the doctrine is a complete, universal solution to various types of infringing content, but that it could provide for a major, composite improvement to the challenges they pose.

There are several key arguments in favour of endorsing the specified request approach over its blunt expectation counterpart. Firstly, there is the advantage in efficiency, a crucial concept for effectiveness in this branch of law making. Within the blunt expectation doctrine, each ISSP is required to deal with the infringements on its own, to design, implement and operate the procedures aimed at tackling various kinds of infringing content appearing on its platform. On the other side, the nature of the specified request doctrine enables a scenario in which resources dedicated to devising and updating the anti-infringement measures are "pooled", for e.g., within a single, proficient organisation responsible for this task, whether through an investment of public funds, or by an additional, proportional tax for online intermediaries reflecting the lifted burden. While each intermediary might be different in terms of its architecture, centralisation of the design process (conducted with a degree of cooperation with the ISSPs) could nevertheless bring about an increase in efficiency, as well as in the quality of the enforcement measures: or at least their core elements. This is advantageous in relation to multiple types of infringing content: as the creation and implementation of enforcement policies incur economic costs t regardless of whether the content is infringing copyright, trademarks, privacy, reputation, etc. - though costs might be higher or lower depending on the legitimate interest involved. It is worth adding that small or start up intermediaries, unable to dedicate the resources necessary for designing and updating their anti-infringement arsenal, might receive a particularly significant benefit in this context.

Another argument in favour of the specified request is a boost in legal certainty, tied to the removal of the mosaic of independent anti-infringement measures endorsed by the ISSPs on an individual basis; a mosaic which is a side-effect of the blunt expectation variant. While there is no express right to legal certainty, it is still a crucial quality of a desirable system of regulation. As Popelier notes, "a person, when making a decision on the basis of certain calculations and expectations, takes into account the legal context. This is possible only when the legal framework is sufficiently accessible to enable a person to take the framework into account". [66] According to Popelier, "(t)he principle of legal certainty is enshrined in the expression "prescribed by law" and similar expressions in other articles of the European Convention on Human Rights". [67] And as for the Charter of Fundamental Rights of the EU, its art. 52(1) states that "any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law (…)".

To demonstrate the presence of legal certainty in the debate surrounding the area of online content regulation; the Council of Europe's recommendation from 2007, focused on cyberspace, urged Member States to establish "the boundaries of the roles and responsibilities of all key stakeholders within a clear legal framework (…)". [68] Furthermore, as Bitton rightly

noted in her critique of the ACTA agreement, general outlines of intellectual property enforcement measures are not sufficient when it comes to online content regulation [69] - and it is argued that this stance extends to the other types of infringing content as well. Finally, legal certainty (convincingly described by the Attorney General in *Scarlet* as a concept descending from the rule of law [70]) had its desired form accurately phrased out by Jones, who wrote that "our sense of predictability should be sourced from legal sources, which would be undermined if the sides of the balancing scales derived their weight from an extensive and unpredictable sample of legal, financial, commercial, ethical, technical or factual elements or justifications". [71]

It is submitted that this undermining scenario gained momentum in the intermediary-oriented sector of online enforcement, largely due to the presence of the blunt expectation approach. Without appropriate synchronisation, a landscape of diverse or diversely formed anti-infringement procedures emerged - a mosaic of procedures and technologies endorsed by the intermediaries wishing to avoid liability for the action of their users. This leads to a significant legal certainty problem. It starts with the notion that it is very difficult for the judiciary to be coherent in assessing whether, according to the law, each intermediary is doing enough to be for e.g., "the diligent economic operator", [72] one escaping liability. It is difficult to find specific, binding guidance in the European jurisprudence (at both Community and Member State levels) on what procedures one should endorse (and in what manner) as an operator of a cyber locker, a streaming website, a blog platform, etc.

The lack of such guidance is of course detrimental not only to the judges, but also to the intermediaries themselves, who struggle to obtain a clear view of what is it that they should do in order to comply with the law; a concern touched upon by Husovec with regard to the application of the negligence rule of liability.[73] A perfect example of a recent case failing to provide the ISSPs' with sufficient information of this kind is the CJEU decision in *UPC Telekabel* [74], warranting the use of broad, effect-based, website blocking injunctions, leaving the ISPs with the task of balancing the human rights involved under the pressure of penalties. The Court's decision has been criticised on the ground of insufficient guidance by multiple academics. Angelopoulos correctly stated that the "ISPs typically want precise orders to be laid out - they are much less eager to attempt to read that mind of the courts and apply guesswork regarding the legal rights of others, especially when their assessments will be subject to re-evaluation by the actual judicial authorities and a potential coercive penalty for themselves if they misgauge the balance": [75] the balance between their steps' effectiveness and these steps' impact on the human rights of users and ISSPs themselves. Hence, the *UPC* case leaves "all intermediaries except those whose case is identical to those already adjudicated in the dark concerning their rights and obligations". [76] Husovec wrote that "the court only delays the problem and creates a great deal of legal uncertainty that could have been prevented by rejecting, or at least limiting, the website-blocking injunctions in the main proceedings". [77] Finally, following James - "(w)hile the UPC decision gives ISPs more freedom and flexibility to take their own steps to address infringing content, many ISPs would probably prefer to be subject to a specific injunction which tells them exactly what they must do rather than risk falling short of what the court requires". [78]

On the other side lies the specified request approach. With its drive towards specification (reinforced by parting with the intermediaries' direct liability for users' infringements, for the sake of liability for non-compliance with the identified requirements), the overall degree of legal certainty is likely to be significantly enhanced. The judges could know exactly which procedures an intermediary has to implement, depending on the service it is running. For example, an operator of an auction site such as eBay, or of a file-hosting website such as

Rapidshare could be required to operate specified, detailed forms of the notice and takedown scheme, of content filtering, as well as of procedures tied to the identification of infringers. Admittedly, then comes the questions of whether the said intermediary is properly implementing the specified requirements, but these are a lot more tangible than their more generic counterparts emerging from within the blunt expectation doctrine.

A further problem which developed within the blunt expectation approach is that a single activity of an intermediary can often fall under more than one ground of liability - and it might be exceedingly difficult to predict which one of them is going to be relied on by the rightsholders or the prosecution (a particular concern at the European Union level). If we consider an operator of a streaming website which is used for copyright-infringing purposes as an example; in the UK, he might become subjected to joint tort liability, [79] authorisation liability, [80] liability for communication to the public, [81] conspiracy to defraud, [82] and criminal copyright infringement; [83] and this list might not be a conclusive one. While this difficulty is not inherent to the discussed approach to intermediary liability, it is one which emerged within it, and one which could be remedied by the endorsement of the specified request approach, setting out a unified, precise list of procedures to be implemented by each fitting category of online intermediaries.

Another principle which is given more adequate attention by this approach is the freedom to conduct a business, protected by Article 16 of the Charter of Fundamental Rights of the European Union. [84] Most enforcement measures aimed at removing access to infringing content in cyberspace place some kind of a burden on the online intermediaries; however, it is a burden which should - following Article 16 of the Charter - be reduced as far as it is feasible. The blunt expectation approach, relying on broad, effect-based demands, carries the risk of placing very significant, potentially unlimited strains on the ISSPs' resources. A generic result of "preventing one's service from being used for infringing purposes" might sound appealing, but in practice, the route leading to it might carry a considerable infringement of the right set out in Article 16 of the CFREU - a threat recognised in both *Scarlet* and *Netlog* cases. [85] Furthermore, writing in the context of ISP blocking injunctions, the Advocate General Cruz Villalón stated that "(n)o [fair] balance can be said to exist in the case of an outcome prohibition not specifying the measures to be taken, which is issued against an ISP". [86] At its core, this line of reasoning can be expanded to other categories of ISSPs, and to other types of illicit content.

The specified request approach is likely to significantly reduce the risk of unlimited burden, and given the corresponding consideration process required for the implementation of this approach, it might carry a lower risk of unjustly burdensome demands being made of the intermediaries. Additionally, the earlier mentioned notion of legal uncertainty suffered by the intermediaries (with the blunt expectation approach) can also be seen as going against the freedom to conduct a business, as pondering the perpetual question of "am I doing enough?" is likely to be resource-intensive in itself, due to the expertise it requires. This burden is particularly exacerbated whenever punitive measures linger behind the "wrong" answer, as noted by Husovec [87] and Angelopoulos. [88] The doctrine furthered by this paper is likely to mitigate the impact on this human right as well, in the same manner as described above in relation to the general legal certainty argument.

Finally, a major, organised shift towards the specified request could be seen as an opportunity for the creation of a more effective legal enforcement framework, one giving due attention to human rights at the design stage, thus providing better awareness and control over the impact of enforcement schemes on rights such as (among others) freedom of expression, right to

privacy and the freedom to conduct a business. And on occasions where effectiveness clashes with human rights, the shift could provide a further opportunity to find a better balance between the two policy goals.

It could be argued that centralising the design of the enforcement procedures endorsed by the ISSPs could expose the specified request approach to a certain weakness, based on the idea that implementing a uniform set of measures which the intermediaries would be required to adopt could facilitate the circumvention efforts of the infringers wishing to for e.g., bypass a website blocking injunction, or confuse a preventive filtering system or avoid identification on a P2P network. This is a concern which, without doubt, ought to be taken into account within such a reform. Nevertheless, it seems that even with this risk, specified request is still more appealing than the blunt expectation approach. To provide an example; concentrating resources on designing and updating a closed set of deeply sophisticated filtering technologies is likely to lead to the development of filters which can be bypassed only by a small amount of fairly proficient infringers, with the vast majority of users being prevented from accessing the infringing content. And from the effectiveness perspective, this would arguably be a much more acceptable situation than the one in which circumvention methods are simpler and more easily accessible - the latter being the *status quo* verified by studies conducted by Adermon and Liang, [89] Lodder and Meulen, [90] van der Ham et al, [91] as well as Clayton. [92] It seems plausible to agree with O'Sullivan, who wrote that "the reality remains that (1) circumvention measures are easily accessible; (2) limited technical skill is required for use; and (3) use demonstrates that internet users are not discouraged by complicating factors". [93]

Hence, it is argued that the specified request approach excels over the blunt expectation approach by centralising the resources used for devising the best possible anti-infringement measures, tackling the "mosaic of measures" and "am I doing enough?" problems for legal certainty, reducing the threat to the freedom to conduct a business, as well as providing an opportunity to improve and maintain the adequate balance between all human rights involved. The risk of facilitating circumvention as a result of harmonisation exists, but it is nevertheless likely to outweighed by a larger, overall improvement in effectiveness.

4. IMPLEMENTING THE SPECIFIED REQUEST APPROACH WITHIN THE EUROPEAN UNION

The Digital Single Market communication document (laying out the EU Commission's agenda for the digital environment) states that "(t)he Commission will launch before the end of 2015 a comprehensive assessment of the role of platforms, including in the sharing economy, and of online intermediaries, which will cover issues such as (…) how best to tackle illegal content on the Internet". [94] It is clear that if the specified request approach is to be chosen as the more appealing reply to this challenge, a series of complex, crucial questions have to be answered first.

4.1. THE CORE IDEA FOR IMPLEMENTATION

The first, and arguably the most important one is: how should this shift be implemented? Who should decide on what steps and procedures are appropriate for each intermediary? Leaving it entirely to the stakeholders involved is unlikely to provide desirable results, due to the perfectly understandable fact that they are motivated by their own interests. Leaving it to the judges, who are only able to act on a case-by-case basis, is not convincing either - and as

Husovec succinctly put it, "it is unrealistic to hope that courts will ever be in a position to completely see the full costs and benefits of the proposed measures. The parties are generally better positioned than courts to make such estimates since they possess private information about their costs and benefits, which the courts first somehow need to acquire". [95]

Instead, this article argues in favour of establishing a dedicated EU-wide body, a "specified request agency", which would be in charge of designing and continuously updating the specific requirements - in cooperation with the relevant private parties - as well as operating a compliance procedure, described below. This way, the concern that in the online regulation area, "any statutory schemes are quickly outdated, and very slow to deploy" [96], would be largely resolved. Such a body should arguably be developed in two tiers - firstly, as an advisory body, obtaining the required expertise and standing; and secondly, as a regulatory body with powers and duties derived from the adequate changes to the EU law.

As for the institutional origin of this agency, there are two primary options. It would either be a completely new body, dedicated entirely to operating the specified request system, or a body derived from one of the existing organisations. Examples of the latter could include the European Observatory on Infringements of Intellectual Property Rights (hereafter referred to as the Observatory; with its scope expanded beyond the IP laws), the Internet Watch Foundation [97] (hereafter referred to as the IWF) or one of the existing Directorates General of the EU Commission (from which a section focused on the specified request approach would be derived). While the IWF has a significant amount of experience in working with intermediaries, providing website blacklists to search engines, its suitability is undermined by its focus on a single, very distinct category of illicit content (child sexual abuse) and institutional nature of a charity registered in the UK. As for the other two; on one hand, the EU Commission's mandate, existing infrastructure and the need to reconcile its regulatory activity in the area of online enforcement with the functioning of the specified request system, seem to make it more appealing. On the other hand, the Observatory has a highly relevant, third party profile and it was actually indicated in the Commission's report on the counterfeit Memorandum as an organisation which should assist non-signatories in adapting their practices to combat counterfeit; [98] an activity matching those desired of the body in charge of the specified request system. Due to the time and space constraints, it is not possible to indicate at this stage which of the three organisations would be best suited to become the required institutional centre: however, it is evident that making the right choice in this regard would be essential for the success of the specified request reform within the EU.

4.2. CHOOSING THE APPROPRIATE STEPS AND PROCEDURES

This leads to the next, equally important question - what exactly should we request of various categories of online intermediaries, in relation to various types of infringing content? Answering this question in a satisfactory manner is likely to require a large scale, dedicated, pan-European research effort in itself; and this article refrains from trying to offer an incomplete list of such obligations. Instead, what it offers is a set of guiding principles to be taken into consideration when attempting to specify the steps and procedures which ought to be implemented by the intermediaries in the struggle against various types of infringing content in cyberspace.

The first key idea of this kind is that the wheel does not need to be reinvented; it is very possible that the crucial majority of procedures and steps which ISSPs could be asked to implement should be based on the already established enforcement schemes. While such schemes could arguably be shaped and implemented in a better, more precise way (an

underlying idea of this paper), it is not really feasible to pull a new online enforcement landscape out of a proverbial hat; though flexibility towards any novel approaches to enforcement should accompany the specified request framework's development.

Secondly, it should be recognised - given the discussion of the freedom to conduct a business in section 3 - that an obligation which can be seen as reasonable for a large intermediary with plenty of resources might not be so for its smaller/start up counterpart - as Husovec noted in the context of website blocking injunctions. [99] One way in which this issue could be accommodated within the specified request system would be to rely on the definition(s) of small and medium enterprises (hereafter referred to as SMEs), set out in the Commission's recommendation from 2003. Its article 2 defines SMEs as "enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million".[100] Small enterprises are defined as those which employ "fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million", [101] and the last category, microenterprises, are defined as those employing "fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million". [102] The specified requirements could be curtailed/softened for the ISSPs matching one of the three categories. Additionally, criteria tied to the online setting (such as the amount of traffic received by a website) could also be involved in this mitigating exercise. Nevertheless, not all obligations should necessarily be adapted in this manner.

Thirdly, every stakeholder group's interests and human rights should be taken into account when designing the specified requirements; this idea is especially worthy of reiterating at this point. According to Ramalho's study, examining (among others) the degree of protection granted to various stakeholders by the EU copyright law, "even though the exact margins may vary, the results show an EU copyright legislation that is partly industry-influenced, while other players seem to have fallen behind". [103] While examining the merits of this conclusion is outside of this article's scope, it is clear that no category of stakeholders should be left behind when designing the obligations of intermediaries, for all content areas.

Fourthly, while this paper focuses on the issues and challenges shared by the legal responses to various categories of infringing content, it has to be remembered that the specified requirements should take into account the differences between those categories and be designed accordingly, in order to avoid harmful side effects. Due to the significance of this concern, it is worth discussing it on the example of a specific enforcement mechanism, namely the notice and takedown procedure. There is a danger that if the specified request system was to embrace a uniform, fully content type-neutral notice and takedown procedure, negative consequences could arise with regards to this measure's effectiveness, human rights impact and more. This risk was explored in depth by Senftleben,[104] in the context of copyright and trademarks - content areas which could be seen as very close to each other, due to both of them being intellectual property rights. However, as Senftleben rightly notes, the two rights differ significantly when it comes to the aim and nature of the protection they offer. Copyright offers more direct protection from acts such as unauthorised reproduction or communication of the work to the public. Trademark law, on the other hand, is more contextual in nature and does not protect the registered sign *per se*; the sign must be used in the course of trade [105] and as Senftleben writes, "(t)rademark protection only concerns particular trademark functions, such as the (…) identification function, the quality function and the communication function". [106]

Hence, copyright offers a broader monopoly than even a well-established trademark with a reputation behind it. [107] This can be justified by the lack of need to provide brand designers and owners with the same incentive to create as the authors of intellectual creations protected by copyright. [108] Consequently, "(a) horizontal notice and takedown standard covering both copyright and trademarks will therefore inevitably be either too low a threshold to reflect the limits of trademark protection (…) or too high a threshold to encompass the more general rights granted in copyright law (…)". [109] Furthermore, the different sets of exceptions present in copyright and trademark laws exacerbate the problem, with the latter containing more contextual exceptions as well (for example, the right to resell, or the right to inform about one's services). [110] According to Senftleben, a trademark-focused notice and takedown procedure has to take into account both the scope/aim of protection and the exceptions peculiar to this content area. [111] And while further comparative work of this kind cannot be conducted in this section due to the time and space constraints, the need to make such distinctions is likely to apply to the other content-type areas and other enforcement mechanisms.

Finally, when designing the specified requirements, the point of balance between over- and under-regulation is very narrow. Mindful of this, the Commission's report on the performance of the Memorandum of Understanding on counterfeit trade submits that the notice and takedown rules "should not be too prescriptive and must include certain mechanisms to deal with abuses of the system. Companies have come up with their own tailor-made methods to address infringements on their online sites".[112] Another example is the efforts aimed at regulation of algorithms present on various online services: as Wagner wrote, such efforts can be "extremely invasive for the companies being regulated, which are being asked to modify what can be considered the core of their business". [113] This article embraces the need to be wary of reaching the purest form of the specified request approach (as described in section 1 of this paper); however, the regulators ought to strive to move as close to it as it is justifiably beneficial and proportionate.

4.3. ENSURING COMPLIANCE

The third key question is one of compliance; if the specified request approach was to be endorsed together with the shift in liability from the users' actions to specific requirements, how should the legal system react to those ISSPs who do not endorse the steps and procedures allocated to them? As Husovec noted, without any sort of liability, the ISSPs are unlikely to take any enforcement actions. [114] Hence, what is proposed is a graduated response system, starting with letters, moving through the severance of revenue streams, with full-scale blocking injunctions and the facilitation of criminal arrests being the last resort measures, reserved for the intermediaries brazenly defying their obligations.

Such a compliance approach would provide a response to the risk of intermediaries "buy(ing) themselves out of their obligations by constantly paying fines". [115] However, it has to be noted that the appropriate discussion of the shape of this path would be of crucial importance, and that the corresponding design process should include input from all of the relevant stakeholders, online intermediaries in particular. Additionally, a robust, efficient appeal procedure at each step of the process would be essential. Otherwise, there would be a significant risk of missing the most required point of balance between being overly punitive and insufficiently effective.

Finally, there is no doubt that the proposed implementation of the discussed enforcement strategy within the European Union would require delivering a careful, detailed answer to

the question of: how should the specified request approach be integrated within the legal framework of the European Union? At this point, it is clear that a challenging, far-reaching reform of instruments such as the E-Commerce Directive, [116] the Information Society Directive [117] and the Enforcement Directive [118] would most likely be essential, together with the enactment of a new Directive responsible for the core elements of the proposed system. Furthermore, the inclusion of the last resort compliance measures, such as arrests, would require an extremely challenging and lengthy harmonisation process, which could encroach on certain aspects of the Member States' substantive laws. European regulation of criminal matters is a tremendously difficult and sensitive matter, as Geiger noted in the context of copyright enforcement measures and the ACTA agreement. [119] This statement is best supported by the unsuccessful attempt to harmonise criminal IP enforcement in the EU through the Second Intellectual Property Rights Enforcement Directive [120] (which was abandoned by the EU Commission in 2010). Nonetheless, it is arguable that the discussed harmonisation aimed at enabling the specified request within the EU, would be distinct from the failed Directive and valuable enough to justify the effort and time needed for its successful completion.

5. CONCLUSION

When attempting to fulfil the online enforcement goals of the Digital Single Market, the EU policymakers are encouraged to centralise their search on the specified request approach. It is, without doubt, a challenging path of legal reform: one which requires a hefty amount of research, discussions and preparations before being implemented. However, small tweaks to the branch of regulation focused on combatting illicit content online are unlikely to bring a noticeable, multifaceted improvement. Sometimes, as the UKIPO report notes, the worthwhile enforcement policy directions might be "challenging and may take the life of the strategy to make real progress". [121] The specified request reform, as presented in this article, has the potential to become one of the most fitting examples of this statement.

---

[1] Researcher at the FREE Foundation (free.org.pl), e-mail address for correspondence: k.k.garstka@gmail.com. The author would like to thank Prof. Paul Torremans, for his insightful comments on the first draft of this article, and Prof. Estelle Derclaye, for her valuable feedback on the ideas discussed within this piece. Thanks are also offered to the anonymous reviewers, for their detailed, enriching suggestions.

[2] Available at https://ec.europa.eu/eusurvey/pdf/survey/33988?lang=EN&unique=bea14714-77ec-4abc-9270-fbe6f6b704b5

[3] See fn. 2, at 17.

[4] A broad term denoting the providers of online services - used in this work interchangeably with "online intermediaries". See art. 2(a) of 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.

[5] *Digital Music Report: Expanding Choice. Going Global* (2012) by IFPI, at 17.

[6] Edwards L, 'Mandy and Me: Some Thoughts on the Digital Economy Bill' (2009) SCRIPTed 6(3), 535, at 537.

[7] Giliker P, *Tort* (2014) Sweet & Maxwell, at 346.

[8] *CBS Songs Ltd v Amstrad Consumer Electronics Plc* [1988] A.C. 1013.

[9] See fn. 8, at 1057.

[10] [2009] EWHC 1094 (Ch)

[11] A VeRO complaint is a complaint made through eBay's notice and takedown scheme.

[12] See fn. 10, at [381], emphasis added.

[13] See fn. 10, at [382].

[14] [2010] EWHC 608 (Ch).

[15] See fn. 14, at [111], emphasis added.

[16] See fn. 10, at [277].

[17] See fn. 14, at [129].

[18] Reed, C (2010), 'Information "Ownership" in the Cloud' Queen Mary School of Law Legal Studies Research Paper No. 45/2010, available at (http://ssrn.com/abstract=1562461), at 250.

[19] [2001] Q.B. 201.

[20] See fn. 19, at 206.

[21] [2007] 1 WLR 1243.

[22] See fn. 21 at [23].

[23] See fn. 21, at [23]. It is a crucial criteria for the purpose of the liability protection regime of the E-Commerce Directive 2000/31. Additionally, it is worth adding that right now, website operators within UK are also protected by section 5 of the Defamation Act 2013, which grants them a conditional safe harbour from liability in defamation.

[24] See fn. 4, Article 14.

[25] The *Myspace* case (2007), Tribunal of Grand Instance Paris, judgment delivered on the 13th of July 2007.

[26] See fn. 25.

[27] [1974] A.C. 819.

[28] See fn. 27, at 840.

[29] (2010) T20087573 (at Middlesborough Crown Court).

[30] See fn. 29, at [8].

[31] Copyright, Designs and Patents Act 1988 c.48, s. 107(2A).

[32] See fn. 31, s. 107(4A).

[33] See http://torrentfreak.com/uk-police-launch-campaign-to-shut-down-torrent-sites-130604/

[34] Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011].

[35] Case C-360/10 *Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) v Netlog NV* [2012].

[36] BGH, 15 August 2013, I ZR 80/12

[37] Digital Millennium Copyright Act 1998, 17 U.S.C. s. 512.

[38] And submerged/shut down towards the end of 2012 - see http://www.bbc.co.uk/news/technology-20540853

[39] [2011] EWHC 1981 (Ch).

[40] 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, rec. 9.

[41] [2012] EWHC 1152 (Ch).

[42] [2013] EWHC 379 (Ch).

[43] [2013] EWHC 2058 (Ch).

[44] [2013] EWHC 3479 (Ch).

[45] [2014] EWHC 3354.

[46] Senior Courts Act 1981 c. 54.

[47] A hybrid blocking system, composed of router-based IP blocking and a form of deep packet inspection focused on blocking URLs. Initially developed to combat child pornography in cooperation with the Internet Watch Foundation. For further information see eg. Clayton R, 'Failures in a Hybrid Content Blocking System' (2005), available at http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf

[48] See fn. 39, at [12].

[49] Mac Sithigh, D (2013), 'The fragmentation of intermediary liability in the UK' JIPLP, Vol. 8, No. 7, at 522.

[50] Though it has to be noted that website blocking orders can also raise subsequent questions for the intermediaries; see section 3.

[51] See fn. 34, at [23].

[52] See fn. 35, at [26].

[53] See fn. 34, at [29] and fn. 35, at [26].

[54] See fn. 34, at [53] and fn. 35, at [51].

[55] See fn. 36, at [60].

[56] *How Google Fights Piracy* report (2013) by Google, at 22, available at https://docs.google.com/file/d/0BwxyRPFduTN2dVFqYml5UENUeUE/edit

[57] *Upgrading the Single Market: more opportunities for people and business* (2015) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2015) 550, at 15

[58] See https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/Pages/Operation-creative.aspx

[59] *Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet* (2011), available at http://ec.europa.eu/internal_market/iprenforcement/docs/memorandum_04052011_en.pdf

[60] See fn. 59, at 3.

[61] See fn. 59, at 6.

[62] See fn. 59, at 6.

[63] See fn. 59, at 5.

[64] See fn. 59, at 3, emphasis added.

[65] *Protecting creativity, supporting innovation: IP Enforcement 2020* (2016), UKIPO, at 20, available at https://www.gov.uk/government/publications/protecting-creativity-supporting-innovation-ip-enforcement-2020

[66] Popelier P, 'Legitimate expectations and the law maker in the case law of the European Court of Human Rights' (2006) 1 E.H.R.L.R, at 10.

[67] See fn. 65, at 10.

[68] Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet, available at https://wcd.coe.int/ViewDoc.jsp?id=1207291

[69] Bitton, M (2012), 'Rethinking the Anti-Counterfeiting Trade Agreement's Criminal Copyright Enforcement Measures' Journal of Criminal Law and Criminology 102 (1), at 116.

[70] Opinion of Mr Advocate General Cruz Villalón in the Case C-70/10, delivered on 14 April 2011, at [67].

[71] Jones, J (2013), 'Internet pirates walk the plank with article 10 kept at bay: Neij and Sunde Kolmisoppi v Sweden' E.I.P.R. 35(11), at 699.

[72] The standard identified in the CJEU limb of *L'Oréal v eBay*, Case C-324/09 *L'Oréal SA v eBay International AG* (2011), at [120].

[73] Husovec M, 'Accountable, Not Liable: Injunctions Against Intermediaries' (2016) (working paper, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2773768), at 32.

[74] Case C-314/12 *UPC Telekabel v Constantin Film* (2014).

[75] Angelopoulos C, 'Are blocking injunctions against ISPs allowed in Europe? Copyright enforcement in the post Telekabel EU legal landscape' (2014) Journal of Intellectual Property Law & Practice, Vol. 9, No. 10, at 818.

[76] See fn. 74, at 815.

[77] Husovec M, 'CJEU allowed website-blocking injunctions with some reservations' (2014) Journal of Intellectual Property Law & Practice, Vol. 9, No. 8, at 633.

[78] James S, 'Digesting Lush v Amazon and UPC Telekabel: are we asking too much of online intermediaries?' (2014) Ent. L.R. 2014, 25(5), at 177.

[79] As laid out in section 2.1.1 of this article.

[80] Set out by Kitchin J in *Fox v Newzbin* as "the grant or purported grant of the right to do the act complained of", not extending to mere enablement, assistance or even encouragement." See fn. 14, at [90].

[81] Based on section 16(1)(d) of the CDPA 1988, which states that the copyrightsholders in the UK have the exclusive right to communicate their works to the public.

[82] As laid out in section 2.1.1 of this article..

[83] As laid out in section 2.1.1 of this article.

[84] The Charter of Fundamental Rights of the European Union (2000/C 364/01), art. 16, stating that "the freedom to conduct a business in accordance with Community law and national laws and practices is recognised"

[85] See fn. 34, at [47] and fn. 35, at [46].

[86] Opinion of the Advocate General Cruz Villalón in the Case C-314/12, at 85.

[87] See fn. 73, at 32.

[88] See fn. 75.

[89] Adermon A and Liang C-Y 'Piracy and Music Sales: The Effects of an Anti-Piracy Law" (2014) Journal of Economic Behavior & Organization (105), 90

[90] Lodder A and Meulen N, 'Discussion of the Dutch Pirate Bay Case Law and Introducing Principles on Directness, Effectiveness, Costs, Relevance and Time' (2012) JIPITEC 4(2), 130.

[91] Van der Ham J, Rood H, Dumitru C, Koning R, Sijm N, De Laat C, Review en Herhaling BREIN Steekproeven (2012), available at https://staff.fnwi.uva.nl/j.j.vanderham/research/publications/dutchpirate.pdf (in Dutch)

[92] See fn. 47.

[93] O'Sullivan K, 'Enforcing copyright online: internet service provider obligations and the European Charter of Human Rights' (2014) 36(9), at 581.

[94] *A Digital Single Market Strategy for Europe* (2015) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2015) 192, at 12.

[95] See fn. 73, at 53.

[96] See fn. 73, at 33.

[97] See https://www.iwf.org.uk/

[98] Report from the Commission to the European Parliament and the Council on the functioning of the Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet (2013) EU Commission, COM(2013) 209 final, at 17

[99] See fn. 77, at 633.

[100] *Commission Recommendation concerning the definition of micro, small and medium-sized enterprises* (2003/361/EC), art. 2(1).

[101] See fn. 100, art. 2(2).

[102] See fn. 100, art. 2(3).

[103] Ramalho A, 'Copyright law-making in the EU: what lies under the 'internal market' mask?' (2014) Journal of Intellectual Property Law & Practice, 2014, Vol. 9, No. 3, at 224.

[104] Senftleben M, 'An Uneasy Case for Notice and Takedown: Context-Specific Trademark Rights' (2012) available at http://ssrn.com/abstract=2025075

[105] See art. 5 of the Directive 89/104/EEC of 21 December 1988 to approximate the laws of the Member States relating to trade marks.

[106] See fn. 104, at 10.

[107] See fn. 104, at 7.

[108] See fn. 104, at 12.

[109] See fn. 104, at 15.

[110] See fn. 104, at 16.

[111] See fn. 104, at 20.

[112] See fn. 98, at 8.

[113] Wagner B, 'Algorithmic regulation and the global default: Shifting norms in Internet technology' (2016) Etikk i praksis. Nord J Appl Ethics, at 8.

[114] See fn. 73, at 12.

[115] See fn. 73, at 42.

[116] See fn. 4.

[117] See fn. 40.

[118] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

[119] Geiger C, 'The Anti-Counterfeiting Trade Agreement and Criminal Enforcement of Intellectual Property: What Consequences for the European Union?', in Rosen J (ed), IP Rights at the Crossroads of Trade (Edward Elgar 2012), at 6.

[120] Amended proposal for a Directive of the European Parliament and of the Council on criminal measures aimed at ensuring the enforcement of intellectual property rights (COM/2006/0168) final - (COD 2005/0127)

[121] See fn. 65, at 33.