WIPO/ACE/12/9 REV. 2
ORIGINAL: ENGLISH
DATE: SEPTEMBER 1, 2017

Advisory Committee on Enforcement

Twelfth Session
Geneva, September 4 to 6, 2017

STUDY ON APPROACHES TO ONLINE TRADEMARK INFRINGEMENTS[*]

Document prepared by Dr. Frederick Mostert, Research Fellow, University of Oxford, Visiting Professor, King's College, London, United Kingdom[**]

ABSTRACT

This study provides an overview of current approaches to online trademark infringements, focusing specifically on possible responses to online sales of counterfeits throughout the world. The study reviews the nature of the global problem of online counterfeits, the common approaches to voluntary measures and the "ratio" principles of intermediary responsibility, the issues of proportionate costs borne by brand owners and platforms, blocking injunctions and other remedies, jurisdiction, the international and cross-border enforcement of judgments, voluntary arbitration, criminal measures, administrative and customs measures, blacklisting and whitelisting. The study also highlights the gaps in the legal measures used in the current online

[*] This study was undertaken with the aid of funds provided by the Korean Intellectual Property Office (KIPO). The Executive Summary is available at: http://www.wipo.int/meetings/en/doc_details.jsp?doc_id=381836.

[**] The views expressed in this document are those of the author and not necessarily those of the Secretariat, the Member States of WIPO or the institutions the author may represent. Apologies for any shortcomings which may remain - the responsibility for which is the author's alone. My gratitude to Sabesh Asokan, LLB (Hons) (First Class), King's College London, founder of King's College London Information Law and Intellectual Property Society, for his tremendously helpful research and contribution to this study. The author is also indebted to the most helpful inputs from Dr. Christina Angelopoulos, Dr. Barbara Lauriat, Mr. Justice Arnold, Professor J. Thomas McCarthy, Professor Paul Goldstein, Professor Bernt Hugenholtz, Professor Graeme Dinwoodie, Professor Ge Jiang, Professor Stacey Dogan, Dr. Knud Wallberg, Terri Chen, Anne Gundlefinger, Jay Monahan, Matthew Bassiur, Nick Wood, Gary Brown, Weizmann Jacobs, Ik Hyun Seo, Alex Urbelis, Dan Bereskin, Dids McDonald, Tim Trainer and Marty Schwimmer.

environment, and synthesizes common international approaches that have emerged to fulfil the need of uniform guidance to the present dilemma.

I. INTRODUCTION

1. The fastest growing counterfeit trade worldwide today is online[1]. In the United States alone, online sales in counterfeit goods reached US$133 billion in 2009[2]. In addition, online counterfeits are expanding well beyond the traditional spheres of individual web-shops and e-commerce platforms to new areas such as social media networks[3]. Not only are big brand owners targeted but small and medium-sized enterprises (SMEs) are also significantly affected in all industry sectors internationally[4]. This poses a serious threat to legitimate businesses, while also putting consumer health at risk and financing organized crime[5].

2. As has been succinctly stated in the Financial Times: "Policing the World Wide Web for an exponentially growing giant wave of counterfeits is a Herculean task. Brand manufacturers chafe at having to commit unlimited time and resources to police auction sites and their growing number of counterfeit listings. Meanwhile, the auction sites claim that filtering everything that comes in and trying to determine what is counterfeit across all industries would be impossible"[6].

3. As anyone in charge of enforcement efforts will attest, the lack of uniform international guidelines has made tackling counterfeits in a borderless digital environment even more challenging. Nonetheless, even though trademarks are territorial, a well-developed set of global, uniform guidelines have, for example, emerged around "famous and well-known marks" during the last 90 years. In this context, WIPO developed and adopted in 1999 voluntary guidelines in the form of the *Joint Recommendation Concerning Provisions on the Protection of Well-Known Marks*[7] which turned out to be of enormous support to Member States throughout the world. Interestingly, in a similar vein, a closer look at recent global developments in intermediary liability and voluntary measures to address online counterfeits points to the gradual emergence of a series of transnational principles, uniform across borders. This is not to deny that substantive differences between jurisdictions remain. However, it is suggested that recognizing these common principles will provide an important first step towards developing consistent, cross-border technical and legal standards.

---

1 WIPO "IP Infringement Online: the dark side of digital" (*WIPO Magazine*, April 2011) http://www.wipo.int/wipo_magazine/en/2011/02/article_0007.html.

2 Ibid.

3 United Kingdom Intellectual Property Office, "Share and Share Alike: The Challenges from Social Media for Intellectual Property Rights" (forthcoming).

4 The European Commission in its 2016 report found an increase in Europe of shipments suspected of violation of IP rights, of which "[s]mall parcels and express and postal traffic resulting from Internet sales make up a significant proportion of detentions" – Commission Staff Working Document on Online Platforms, accompanying the document "Communication on Online Platforms and the Digital Single Market" (COM(2016) 288) available https://ec.europa.eu/digital-single-market/en/news/commission-staff-working-document-online-platforms, 21 (the value of over 35 million detained articles in equivalent genuine products is estimated to be just over €617 million; at fn. 99 referring to Report on EU customs enforcement of IPR – Results at EU border 2014, 2015). Moreover, the OECD in its 2016 report found that the harm to legitimate business is not reserved for big branded businesses, but equally affects small and medium enterprises of all industries – OECD/EUIPO (2016), *Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact* (OECD Publishing, Paris) http://dx.doi.org/10.1787/9789264252653-en, 72, 68 (Counterfeit and pirated trade continues to grow and "that counterfeit and pirated products accounted for as much as USD 461 billion in world trade in 2013" which "amounted to up to 2.5 % of world trade in 2013. This was even higher in the EU context where counterfeit and pirated goods amounted to up to 5 % of imports.").

5 Ibid.

6 Frederick Mostert, 'Counterfeits on Ebay: who is responsible?' (*The Financial Times,* 17 July 2008) https://www.ft.com/content/e694a4fe-5426-11dd-aa78-000077b07658 accessed 16 July 2017.

7 http://www.wipo.int/publications/en/details.jsp?id=346.

4. The prevailing response to online trademark infringement among virtually all WIPO Member States has been to make civil remedies against online infringers available to trademark owners[8]. This has been supplemented by the recognition of primary, accessory or intermediate liability for internet service providers in certain limited scenarios, and voluntary measures adopted by online intermediaries to avoid liability. Yet, the sale of counterfeits online remains commonplace. Existing remedies lack uniform international guidelines and harmonization, limiting their effectiveness in a global digital environment.

5. Moreover, existing solutions are often subject to the following challenges: (1) the identity of the infringers is often unknown to the trademark owner; (2) the anonymity problem exacerbates the "whack-a-mole" phenomenon – where a webpage is taken down, another online listing usually pops under a different URL almost instantly as the infringers themselves evade identification; (3) the sheer volume and velocity of online sales of counterfeits make them very time sensitive – postings are typically posted only for a few hours or days, and this *tempus fugit* issue makes the timely online track and trace of counterfeit listings very difficult; (4) civil remedies are complemented with criminal and administrative measures, but these normally require a large volume of counterfeit infringements in order for government authorities to take action; (5) it is not always clear what minimum contacts or links are required to found jurisdiction in a country; (6) infringers typically use more than one website in different countries which raises *inter alia* questions of enforcement of foreign judgments; and (7) currently there is no international mechanism for the voluntary arbitration of online counterfeit cases.

6. This study seeks to provide an overview of current approaches to tackle online trademark infringement, focusing specifically on the issue of the sale of counterfeit goods online. From the significant research undertaken internationally, it is clear that the sheer volume and range of counterfeit products online is at the heart of the current online dilemma throughout the world.

7. First, the available civil remedies will be examined in Sections II to V. The effectiveness of civil remedies depends on the development and application of consistent technical and legal standards across borders. A key challenge in this area is jurisdictional issues surrounding the enforcement of judgments across borders. This study will assess the scope and limitations of existing and proposed solutions to this challenge, including avenues for judicial co-operation between Member States, and mechanisms to facilitate voluntary alternative dispute resolution mechanisms, including arbitration. Moreover, by exploring existing principles of intermediary responsibility among WIPO Member States, it will be demonstrated that despite a lack of formal legal harmonization, key uniform tenets can be identified internationally. It has been noted that a transnational principle of intermediary responsibility can be distilled from these core common legal approaches, to serve as a vital source of uniform guidance, aligned with existing practice[9].

8. Second, existing criminal and administrative measures will be reviewed in Sections VI and VII. This study will proceed to identify their weaknesses in the online environment, while also highlighting emerging solutions and practices globally.

---

[8] The World Trade Organization (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) sets the minimum civil, administrative and criminal standards of IP protection, but having been signed in a pre-online era its provisions are not "online-specific". States have turned to regional or bilateral treaties in order to further regulate issues of IP, including protection of IP online (e.g. Chapter Twenty (IP), Art. 20.11 of the Canada and EU Comprehensive and Economic Trade Agreement (CETA); Chapter 18 (IP) Art. 18.10, paragraph 30 of the Republic of Korea – US Free Trade Agreement and Confirmation Letter on Limitations to ISP providers of June 30, 2007).

[9] Frederick Mostert and Sabesh Asokan, 'International common approaches to intermediary responsibility'(*Intellectual Property Magazine*, 9 August 2017) http://www.intellectualpropertymagazine.com/trademark/international-common-approaches-to-intermediary-responsibility-125712.htm accessed 9 August 2017.

9. In sum, this study's investigation of these issues reveals that the key tools against online counterfeits – where they exist in Member States – are voluntary measures, cross-border co-operation on enforcement, voluntary arbitration, whitelisting of genuine owners and blacklisting of counterfeiters, effective criminal measures and intermediary liability. These tools are in urgent need of uniform practices as online counterfeiting is a significant commercial, technical and legal issue which transcends national boundaries. Only by developing and applying consistent legal and technical standards can all stakeholders in the international community set up an effective response sensitive to the full breadth of its scope.

II. THE NATURE OF THE GLOBAL ONLINE COUNTERFEIT THREAT

A. COUNTERFEITS ON E-COMMERCE PLATFORMS

10. E-commerce on online marketplaces is increasing exponentially throughout the world[10]. Consequently, counterfeiters are shifting their activities online and distributing counterfeit goods on the World Wide Web. In 2007, the OECD estimated that the global trade in in counterfeit and pirated goods could have accounted for up to USD$250 billion. The value was estimated by the OECD and EUIPO to be US$461 billion in 2013[11] and by 2022, it could reach as high as US$991 billion according to the International Chamber of Commerce[12].

11. There has also been a significant increase in the number of shipments suspected of violating intellectual property (IP) rights within Europe[13]. In 2014 alone, 95,000 shipments were detained by European Union customs authorities, most of which were small parcels and other postal traffic resulting from internet sales[14]. The value of the equivalent genuine products (over 35 million detained articles) is estimated to be over €617 million[15].

B. COUNTERFEITS IN SOCIAL MEDIA

12. A new threat that has emerged is the proliferation of counterfeits on social media[16]. Counterfeits are very openly being touted by counterfeiters on the official social media pages of famous brands. As a recent UK Intellectual Property Office study points out**,** "social media is increasingly a key part of a complex eco-system to divert traffic from authentic sites covering myriad rogue online platforms"[17]. The Facebook, Instagram and WeChat pages of internationally well-known brands have all been subject to this phenomenon.

13. As Jenny Wolfram, CEO of BrandBastion, points out: "during a two weeks' period earlier this year, one brand pirate posted 114 comments, advertising counterfeit goods on the Instagram accounts of many internationally famous brands"[18].

---

10 European Commission (n 4).

11 EUIPO (n 4). See also OECD (n 4).

12 Frontier Economics, 'The Economic Impacts Of Counterfeiting and Piracy' (Commission Report International Chamber of Commerce, Business Action to Stop Counterfeiting and Piracy (BASCAP) and International Trademark Association (INTA), 2017) 8 http://www.inta.org/Communications/Documents/2017_Frontier_Report.pdf accessed 17 August 2017.

13 Ibid.

14 Ibid.

15 Ibid.

16 United Kingdom Intellectual Property Office (n 3).

17 Ibid. Dennis Collopy, Senior Lecturer, School of Creative Arts, University of Hertfordshire (personal communication, July 16, 2017).

18 Jenny Wolfram, CEO, BrandBastion, (presentation, March 22, 2017).

14. Beyond lost sales, counterfeits listings on social media can pose a serious threat to public health and safety. In the United Kingdom, a recent law enforcement operation seized "tens of thousands of counterfeit and unsafe goods including dangerous cosmetics, perfumes, razor blades, electrical products and chargers as well as clothing, footwear, leather goods and tobacco products"[19]. This included "Android TV boxes with unsafe mains chargers, to several hundreds of counterfeit Cinderella dolls containing high levels of toxic phthalates" [20]. As National Trading Standards points out, "fake goods are not subject to the stringent safety checks that genuine goods, made by legitimate businesses, must comply with"[21].

15. In addition, counterfeits listings on social media inflict serious reputational harm on brands. Customers of the genuine brand are confused by listings that piggyback onto the genuine social media pages of brands, and are tricked into buying a fake product. These disgruntled customers, in turn, post their own very damaging remarks about the brand on the same media page for all other customers to see.

16. Counterfeiters have also established dedicated replica storefronts on social media platforms such as Facebook possibly to evade more stringent measures against counterfeiting increasingly being adopted by online e-commerce platforms such as eBay and Alibaba[22].

III. THE *IUS GENTIUM* OF VOLUNTARY MEASURES – INTERNATIONAL COMMON APPROACHES

17. In response to an increase in online sales of counterfeit products, online intermediaries and right holders have, to some extent, engaged in voluntary co-operation[23], which has proved to be successful, albeit not fully effective, in stopping online counterfeit sales. These measures are either designed by online intermediaries themselves[24], drafted in co-operation with rights holders[25] or supported by states and their administrative authorities[26].

---

19 National Trading Standards, 'Products Worth Millions Seized in Counterfeiting Crackdown' (23 December 2016) http://www.nationaltradingstandards.uk/news/products-worth-millions-seized-in-counterfeiting-crackdown/ accessed 1 August 2017.

20 National Trading Standards, 'Landmark crackdown on social media counterfeiting and piracy launched' (24 June 2015) <http://www.nationaltradingstandards.uk/news/landmark-crackdown-on-social-media-counterfeiting-and-piracy-launched/> accessed 1 August 2017.

21 Ibid.

22 See para [28]-[34] in this study.

23 Frederick Mostert, "Fakes Give Alibaba Chance to Turn Crisis into Opportunity" (*Financial Times*, 8 June 2016) https://www.ft.com/content/d838b4fc-2698-11e6-8ba3-cdd781d02d89 accessed 16 July 2017. See also Mostert (n 6).

24 EU Intellectual Property Office, "Study on Voluntary Collaboration Practices in Addressing Online Infringements of Trade Mark Rights, Design Rights, Copyright and Rights Related to Copyright" (September 2016) (hereinafter EUIPO Study 2016). The main authors of the study are: Prof. Dr. Thomas Hoeren; Prof. Dr. Guido Westkamp; María Vidal, Susana Rodriguez Ballano, Paula Iun, Ana De Lluc Compte, Jaime Pascual, Andrea Sánchez Guarido and Julia Torres.

25 Presented in WIPO, Advisory Committee on Enforcement: C. Aubert "The Activities of the Federation of the Swiss Watch Industry in the Area of Preventative Actions to Address Online Counterfeiting" (31 July 2015) WIPO/ACE/10/22.

26 In China, Administrative Measures for Online Trading (State Administration for Industry and Commerce, 2014) in Art. 6 encourage online commodity dealers and relevant service providers to form industry organizations and conventions, to promote industry self-discipline. On EU level, Art. 16 of the E-Commerce Directive stipulates that member states and the European Commission will promote the development of codes of practices among trade, industry and consumer organizations; similarly Art. 17 of the Enforcement Directive on codes of practices to prevent IP infringement. This led to a signing of Memorandum of Understanding on the Sale of Counterfeit Goods (signed on 4 May 2011, now revised and open for signature since 21 June 2016) – EUIPO Study 2016, 16.

18. As has been noted[27], in effect, a *ius gentium* of common principles or international common approaches have emerged. Such joined-up principles can be uniformly observed in the transnational approaches to voluntary measures that this study will proceed to highlight in more detail. This is aligned with calls, such as that by Knud Wallberg, for the development of a code of conduct for voluntary measures relating to counterfeit goods in the context of the cross-border, multi-jurisdictional environment of digital marketplaces[28].

19. First, online intermediaries have developed initiatives to voluntarily remove counterfeit listings upon notification through policies such as "notice and take down". Second, intermediaries have voluntarily engaged in extensive proactive monitoring of uploaded listings using key words and other indicia. Thus, when products are offered – particularly in certain categories – the software identifies the use of certain key words, such as "faux", "fake" and "look alike", and flags these items for immediate review. Third, intermediaries have adopted filtering systems that use algorithms to automatically remove and prevent counterfeit listings from being displayed (digital fingerprinting). Fourth, intermediaries have adopted a "follow the money" approach to tackle online infringement, and introduced measures to target payment processors for online traders who engage in the sale of counterfeit goods[29]. In some instances, intermediaries have, as a natural next step to tracing the money, also followed through with "notice and track-down" measures to help right holders to find the sellers of counterfeit products and stop the problem at source. Fifth, voluntary registry systems have been implemented to enable right holders to control how product listings featuring their trademarks can be displayed online – this includes being able to limit listings to a pre-approved list of sellers[30]. In addition, these registry systems serve as prima facie evidence of rights ownership, facilitating the speedy take-down of counterfeit material when rights holders submit take-down notices. Sixth, advertising codes of practice have been developed to discourage illegal content online. This is accomplished by preventing advertisements from being displayed on counterfeit websites ("advertising misplacement"), cutting off advertising revenue[31]. Last, intermediaries have also engaged in the education of users and businesses through educational campaigns, and at the time of uploading[32].

A. NOTICE AND TAKE-DOWN PROCEDURES

20. "Notice and take-down" policies (used for example by Alibaba[33], Auction, eBay, Gmarket, Interpark, Rakuten or 11th Street) allow for right holders to notify an infringement of their IP rights and the intermediary to take down listings of counterfeit products. Many of these notice and take-down practices were initially developed in response to copyright infringements[34] but

---

27 Mostert and Asokan (n 9).

28 Knud Wallberg, "Notice and Takedown of Counterfeit Goods in the Digital Single Market: A Balancing of Fundamental Rights" [2017] *Journal of Intellectual Property Law & Practice*.

29 US International Anti-Counterfeiting Coalition (IACC) payment processor initiative and portal program, later named RogueBlock – EUIPO Study 2016, 14, 23–24. See "The Canadian Anti-Fraud Centre's Project Chargeback: Leading the Charge(Back) Against Fakes!" in WIPO/ACE/11/8.

30 However, these efforts have been hampered by legal uncertainty regarding the compatibility of these measures with competition law.

31 Austrian Ethics Code for the Advertising Industry (2014); UK principles of good practice of the trading of digital display advertising – EUIPO Study 2016, 14, 19–23. See WIPO/ACE/10/21 on Interactive Advertising Bureau (IAB) Poland's initiatives. In EU similar practices have been initiated in Austria, Denmark, France, Italy, the Netherlands, Poland, Slovakia and the UK.

32 For instance, individuals who attempt to list an item that contains a particularly sensitive brand name and/or a key word, such as "faux", will be presented with a warning message regarding the sale of counterfeits as a deterrent.

33 Presented in WIPO, Advisory Committee on Enforcement: N. Liang "Intellectual Property Protection Practices of Alibaba Group under the Internet Platform-Based Business Model" (12 February 2014) WIPO/ACE/9/24.

34 Marsoof has explored notice and take down measures in the copyright context and tested their potential abuse in order to propose a more suitable framework in the trademark context – A. Marsoof, "Holding Internet Intermediaries

were subsequently extended to trademarks. Such industry practices have also been encouraged by the authorities in Denmark, France, the Netherlands and the EU, through the adoption of "voluntary collaboration practices"[35].

21. As the illegal content can quickly pop up and reappear elsewhere online after the initial take-down (commonly referred to as the "whack-a-mole" dilemma on the internet), right holders are concerned that the notice and take-down procedure fails to adequately protect their rights. Counterfeiters are more adept at using new technologies than those trying to shut them down. This has turned the fight against counterfeit sites into a "whack-a-mole" game. Take down a counterfeit page and an identical one pops up in a new location[36]. Moreover, the onus is on the right holder to continuously monitor the internet, incur the costs of gathering evidence and serve a new notice and take-down order for each case of infringement. Arguably, this is a cumbersome process for right holders – and is likely to be particularly detrimental to those right holders (especially SMEs) with limited resources. In addition, take-down notices can be challenging to administer for online intermediaries, especially when faced with multiple and rapid requests for take-downs.

22. Some intermediaries are, however, taking steps to make the notice and take-down process work better. For instance, processes to submit take-down notices can be streamlined[37], and potentially counterfeit listings can be proactively flagged for review by right holders[38]. In addition, right holders who have a proven track record of submitting legitimate take-down requests could be given presumption of good faith, and enjoy an expedited take-down submission process[39].

B. NOTICE AND STAY-DOWN PROCEDURES AND FILTERING

23. Filtering services, particularly inasmuch as they would be the duty of an intermediary to set up specific software to seek and identify online infringements, have been controversial. Where a filtering service seeks to impose a general monitoring obligation, it has been deemed to be unlikely to meet the test of proportionality and is therefore not available as a remedy[40]. However, filtering might be ordered as a response if it does not impose a general monitoring obligation[41]. For instance, the German Federal Court of Justice decided in Rapidshare (Alone in the Dark)[42], that while Rapidshare did not have a duty to perform proactive monitoring of the files uploaded by its users, deleting infringing content after being notified by copyright holders

---

Accountable for Infringements of Trademark Rights: Approaches and Challenges" (PhD thesis, King's College London, 2016).

35 French Charter for the fight against the sale of counterfeit goods on the internet between IP rights holders and e-commerce platforms; the Dutch notice-and-take-down code of conduct directed at ISPs that provide a public telecommunications service in the Netherlands; the Danish code of conduct for ISPs regarding the management of court DNS blocking orders regarding IP infringement – see EUIPO Study 2016, 14, 19–23. Article 16 of the E-Commerce Directive and Article 17 of the Enforcement Directive.

36 Frederick Mostert, 'Counterfeits on Ebay: who is responsible?' (*The Financial Times,* 17 July 2008) https://www.ft.com/content/e694a4fe-5426-11dd-aa78-000077b07658 accessed 16 July 2017.

37 Alibaba has facilitated the submission of take-down notices by developing a one-stop website (https://ipp.alibabagroup.com) for IP owners to register, submit their IP and file complaints for, e.g., trademark, copyright (e.g. image theft) and patent infringement.

38 Alibaba's IP Joint Force System (IPJFS) is one example.

39 Examples include the IACC MarketSafe® Program and Alibaba's Good Faith Program.

40 See for example, the case of CJEU *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (Judgment, 24 November 2011) Case C-70/10, ECLI:EU:C:2011:771.

41 Christina Angelopoulos, European Intermediary Liability in Copyright: A Tort-Based Analysis, (Kluwer Law International, 2016) 158-160.

42 BGH, *Rapidshare I,* 12 July 2012, I ZR 18/11.

was not enough[43]. Rapidshare had to go further and perform searches for future infringements of the notified content, as well as take all "reasonable measures" to make sure users could not proceed with such infringements in the first place. This could include automatic word filters supplemented by subsequent manual controls[44].

24. Other filtering procedures, such as "notice and stay down"[45], have also been proposed. Notice and stay down involves an online intermediary voluntarily taking steps to make certain illegal content unavailable by blocking access to it and monitoring its own digital space for any subsequent reappearances of that content – which it will have to block again – for a specific period of time. Notice and stay down is currently being debated at EU level[46]. Whilst right holders gain certainty that their rights are protected (at least for a specific period), online intermediaries would have to voluntarily incur the significant financial and human-resource costs involved in an effective system of monitoring and blocking. For instance, intermediaries would have to elect to install filtering technology, and to expend resources to update that technology on an ongoing basis. In particular, in the case of small or medium sized ISPs, such financial and technical resources required could be prohibitive.

25. Right holders may view notice and stay down as a "magic wand" solution, but it also raises issues of free speech and access to information (in particular if large amounts of content are blocked) and privacy concerns stemming from ISPs monitoring the activities of their customers. Notice and stay down may be disproportionately onerous on intermediaries and fails to address the heart of the problem, i.e. the source: the counterfeiters themselves. Consequently, in France, the Court of Cassation effectively put an end to judge-imposed notice and stay down procedures[47]. The court held that the core feature of notice and stay down – a requirement that intermediaries prevent the reappearance of content they have already removed – would likely be equivalent to imposing a general monitoring obligation which is prohibited by Article 15 of the E-Commerce Directive[48]. However, German decisions have demonstrated a willingness to allow stay-down as evidenced in the *Internetversteigerung* and *Rapidshare* cases, in contrast to the skepticism of French courts[49].

26. Some platforms have put in place extensive proactive take-down programs, i.e. programs in which the platform itself monitors and removes listings, without the need for a take-down request from a right holder. For example, Alibaba's proactive monitoring team employs hundreds of monitoring models and it has adopted new technologies such as optical character recognition to detect counterfeits at a lower cost[50].

---

[43] Christina Angelopoulos, European Intermediary Liability in Copyright. A Tort-Based Analysis, (Kluwer Law International, 2016) 159.

[44] Ibid.

[45] The duty of an intermediary to monitor its digital space for reoccurrence of infringing content is continuously examined at EU level http://ec.europa.eu/internal_market/e-commerce/notice-and-action/index_en.htm.

[46] http://www.ec.europa.eu/eusurvey/runner/Platforms.

[47] Catherine Jasserand, "France: the Court of Cassation Puts an End to the Notice and Staydown Rule" (*Kluwer Copyright Blog*, 14 August 2012) http://kluwercopyrightblog.com/2012/08/14/france-the-court-of-cassation-puts-an-end-to-the-notice-and-stay-down-rule/ accessed 16 July 2017.

[48] Graeme Dinwoodie, *A Comparative Analysis of the Secondary Liability of Online Service Providers* 3, 45 (Springer, Dinwoodie ed., 2017). See also Christine Gateau and Pauline Faron, "Take Down, Stay Down: Paris Court of Appeal Confirms Hosting Providers Have No General Monitoring Obligation", 20 *Computer & Telecomm. L. Rev*. 12 (2014).

[49] See *La société Google France c. la société Bach films* (L'affaire Clearstream) (11-13.669), Cour de cassation, 12 July 2012; *La société Google France c. La société Bac films* (Les dissimulateurs) (11-13666), Cour de cassation, 12 July 2012; *La société Google France c. André Rau* (Auféminin) (11-15.165; 11-15.188) Cour de cassation, 12 July 2012).

[50] Alibaba has the capacity to process 100 million pieces of data per second, which enables it to conduct proactive scans of 10 million product listings a day. In 2016, the number of listings proactively detected and removed by Alibaba was 26 times greater than the number of listings removed by Alibaba in response to complaints submitted by all IP right holders combined http://www.alizila.com/alibabas-big-data-means-counterfeiters-can-run-cant-hide-ipr-enforcement/ accessed 1 August 2017.

C. NOTICE AND DISCLOSURE PROCEDURES, NOTICE AND TRACK-DOWN

27. Notice and track-down measures have also been introduced in China and the UK with some success. Notice and track-down measures provide for the disclosure of the contact details of the online seller of the counterfeit products. This measure has proven to assist the right holders successfully to track the actual origin of the counterfeits and to stop the problem at source. Most recently, these measures were adopted in China, where the Circular of the Ministry of Commerce imposes several duties on the online intermediaries and e-commerce operators. This includes the duty to "improve accessibility to information on sellers, payments details, logistics, after-sale service, dispute resolution, compensation, process monitoring"[51]. These measures are also reiterated in the Administrative Measures for Online Trading (State Administration for Industry and Commerce of China, 2014). In the UK in similar vein, the Intellectual Property Minister made a policy announcement in 2016 on notice and track-down, committing more efforts in battling online piracy and counterfeiting[52].

D. CONSTRUCTIVE COLLABORATION – ADOPTING INNOVATIVE TECHNOLOGICAL SOLUTIONS

28. Policing the World Wide Web for an exponentially growing giant wave of counterfeits is a Herculean burden to shoulder alone[53]. Brand owners chafe at having to commit vast resources to policing online platforms. Platforms protest that filtering every transaction and trying to determine what is counterfeit across all industry sectors is mission impossible. To effectively confront the online counterfeit problem, it is imperative that brand owners and intermediaries work together and share the responsibility to stop fakes, while at the same time avoid stifling innovation and new ways of engaging in trade.

29. Some intermediaries and right holders who jointly recognize this imperative have collaborated constructively to explore new ways to stop online sales of counterfeits. An early pioneer in this area was eBay. eBay ceaselessly monitored seller listings and put extraordinary resources into developing cutting-edge tools and strategies. This included introducing possibly the first notice-and-take-down procedures for trademark violations, spearheading the use of voluntary proactive monitoring using keywords and applying "red flag" standards, adopting stringent measures against repeat offenders and – crucially – maintaining fast response times (usually within hours) to take-down notices. These methods were revolutionary then and still provide the gold standard for online retailers.

---

[51] The Ministry of Commerce, the Ministry of Industry and Information Technology, the Ministry of Public Security, the People's Bank of China, the General Administration of Customs, the State Administration for Industry and Commerce, the General Administration of Quality Supervision, Inspection and Quarantine, the General Administration of Press and Publication (National Copyright Administration) and the State Intellectual Property Office jointly released a "Circular of Further Pushing Forward the Crackdown on Intellectual Property Right Infringement and Manufacturing and Sale of Passing-offs and Inferior Products in the Online Shopping Sector" – Ferrante, "E-commerce platforms: liability for trade mark infringement reflections on Chinese courts' practice and remedies against the sale of counterfeits on the internet" (2015) 10(4) *JIPPL* 255; Ferante, 259 (referring to The Circular found on the official website of Ministry of Commerce of People's Republic of China, at http://www.mofcom.gov.cn/article/h/redht/201104/20110407512137.shtml (in Chinese only); and Administrative Measures for Online Trading (State Administration for Industry and Commerce, 2014).

[52] Baroness Neville-Rolfe (10 May 2016) reported at https://www.gov.uk/government/speeches/launch-of-intellectual-property-enforcement-strategy; launching the new IP enforcement strategy in the UK – 'Protecting Creativity, Supporting Innovation: IP Enforcement 2020' available at https://www.gov.uk/government/publications/protecting-creativity-supporting-innovation-ip-enforcement-2020.

[53] Mostert (n 6).

30. Yet, the efforts of eBay and the brands that have worked with eBay to date should act as a benchmark for others and not as a ceiling. More needs to be done, especially as counterfeiters are often more adept at using new technologies than those trying to shut them down. Recognizing this, Michael Evans, president of the major online platform Alibaba, pointed out that the platform must adopt "the tools to change the way this war is waged . . . using data and technology . . . to defeat the counterfeiters"[54]. At a meeting in June 2016, a group of British brand owners presented Alibaba with a wish list including notice and track-down, digital fingerprinting and a mechanism to flag and blacklist persistent infringers. Such tracing parallels the fundamental "follow-the-money" principle.

31. Following these constructive co-operation initiatives with British brands, Alibaba has now spearheaded the use of new technologies such as big-data analytics and machine learning, setting a new cutting-edge standard and benchmark for intermediaries in this area. These measures serve to both proactively remove counterfeit listings and to track down the source of counterfeits and the factories where they are produced. For instance, once the automated systems flag a product as counterfeit, the system is able to pool information such as account information, shipping and return addresses, related accounts and payment processor information. Next, the system is able to intelligently parse this information to identify counterfeiters, as well potentially revealing the manufacturing source by tracing the movement of funds. Alibaba's initiative has already borne fruit. By sharing information gleaned from these tools with law enforcement officials in China, authorities have seized counterfeit goods worth RMB1.43 billion, and eliminated 417 production rackets[55].

32. The online retailer Amazon is also exploring how artificial intelligence and machine learning can help to proactively identify counterfeit items and prevent them from being listed. By automatically scanning information about product attributes such as brand and category, as well as seller information, these tools enable platforms to flag potential counterfeiters and counterfeit products. This is an important development that addresses a perennial challenge in removing counterfeit listings (the ubiquitous "whack-a-mole" issue on the web): the ease with which counterfeiters (and especially repeat offenders) can re-list counterfeit products makes policing platforms burdensome both financially and in terms of labor. Thus, these automated tools help to augment the efforts of brand owners and platforms who have relied on teams of individuals to manually flag and remove counterfeits.

33. Some e-commerce marketplaces are also taking steps to enhance their IP protection programs through stronger collaboration with right holders. For example, Amazon has created a Brand Registry program. This is a form of whitelisting[56] which gives brand owners the ability to control which sellers are able to list their products, and implements stronger due diligence checks on sellers before they are permitted to list a registered brand. Similarly, Alibaba has developed a comprehensive online rating system to regulate sellers. The system is powered by Alibaba's data-processing engine and users are evaluated based on the following metrics – identity verification results, user credibility assessment, compliance with platform policies, penalty records, positive user behavior, collaboration efforts, and others. This rating system enables Alibaba to enforce its rules and policies in a more targeted manner against counterfeit merchants, hence optimizing overall governance efficiency.

---

[54] Mostert (n 23).

[55] Alibaba, for instance, uses big data algorithms to identify, block, and remove misleading uses of product identifying language. Listings identified by the initiative are subject to takedowns, lowered merchant credit ratings, and suspension of marketing activities. http://www.alizila.com/alibabas-big-data-means-counterfeiters-can-run-cant-hide-ipr-enforcement/ accessed 1 August 2017.

[56] See also para. 120 below.

34. Second, a recent voluntary enforcement initiative between the Motion Picture Association of America (MPAA) and two online registry operators in the copyright context could potentially be applied to tackle the sale of online counterfeit goods (albeit that the nature of the counterfeit or pirated products may differ). Titled the "trusted notifier" program[57], take-down notices submitted by the MPAA are presumed to be credible and are processed on an expedited basis. While this has raised freedom of speech concerns in the copyright context[58], such concerns are mitigated with respect to counterfeit goods – especially where it is clear the goods are counterfeit and there is no countervailing free-speech issue as deceptive speech is not considered to be protected speech[59.] Therefore, such a program would be a valuable asset to responding more expeditiously to the rapid proliferation of counterfeit websites online.

35. However, it is important to note that technological innovations such as artificial intelligence and machine learning are not a silver bullet to solving the counterfeit problem. As Jay Monahan points out, trademark infringement is inherently different from copyright infringement and potentially more challenging to police[60]. Policing copyright infringement relies on identifying unauthorized copies, and this is mainly a matter of finding an exact match or close match on a reference file, which automated systems are adept at.

36. In contrast, trademark infringement occurs in both the underlying product (which is often not available for inspection) and the advertisement or listing. Sophisticated criminals list counterfeits using pictures of the authentic products, real descriptions, and at prices close to the original, making them difficult to flag using automated technologies. For instance, optical image or character recognition technology could be circumvented by counterfeiters who use images of genuine products in their listings.

37. Furthermore, as Terri Chen notes, even rights holders struggle to distinguish between online listings which contain legitimate second-hand or grey goods and counterfeits[61]. Therefore, it is important that overreach be avoided, especially in the context of using automated systems that are in early stages of development and whose accuracy continues to improve over time. Moreover, these measures ultimately fail to address the actual source of the problem: the counterfeiters themselves.

38. In summary, on the crucial point of constructive cooperation, as noted in the Financial Times: "Where do the recent epic legal battles leave web customers who are saddled with counterfeits daily? That there is a plethora of fakes online is glaringly obvious. Who then is responsible for removing the counterfeit products listed on (platforms). As in so many walks of life, the answer lies in the constructive co-operation. The answer for assessing responsibility lies in the middle – both sides should in equal measure diligently confront the online counterfeit problem together. Brand owners and auction sites need to work together and share the responsibility to stop fakes, like wildfire, to avoid a restraint on the progress of society"[62].

---

[57] MPAA, 'Donuts and the MPAA Establish New Partnership to Reduce Online Piracy' (Feburary 9, 2016) http://www.mpaa.org/wp-content/uploads/2016/02/Donuts-and-MPAA-Establish-New-Partnership-2.9.16.pdf accessed 1 August 2017. See also WIPO/ACE/12/10, pp. 32-36.

[58] Annemarie Bridy, Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation (February 20, 2017) *Washington and Lee Law Review*, (Forthcoming). https://ssrn.com/abstract=2920805> accessed 1 August 2017.

[59] Counterfeits as a form of deception qualifies as "deceptive speech" which the US Supreme Court has earmarked as unprotected speech under the First Amendment. See *Friedman v. Rogers*, 440 U.S. 1 (1979).

[60] Jay Monahan, General Counsel, ResearchGate, and former Deputy General Counsel, Intellecutal Property, eBay (personal communication, 7 August 2017).

[61] Terri Chen, Legal Director, Google, (personal communication, 28 July 2017).

[62] Mostert (n 6).

39. The answer for assessing who should bear the cost lies in the middle – both sides should diligently confront the online counterfeit problem together, and share the burden in a manner sensitive to the precise issues at play[63].

E. ADVERTISING CODES OF CONDUCT

40. A key source of revenue for individuals who facilitate the infringement of IP rights online is digital advertising. IP infringing websites often receive high traffic, and this exposure to a large number of users enables them to earn significant sums of as much as €5.3 million each annually. Consequently, right holders and the advertising industry have turned to targeting revenue sources of online infringers by adopting advertising codes of practice to reduce the financial support counterfeiters earn through digital advertising, undermining their commercial viability[64]. For example, a recent WIPO ACE document has highlighted a code of practice developed by IAB Poland[65]. The code encourages advertisers and agencies to use advertising misplacement tools such as whitelists, data sharing of URLs of IP infringing sites and countermeasures used to evade blocking (black-listing), as well as adopting contractual arrangements that state a willingness to restrict the display of advertisements on IP infringing sites[66].

41. Similarly, the Digital Trading Standards Group (DTSG) in the United Kingdom has introduced a series of six good practice principles for the trading of digital display advertising: (1) trading activities of the seller and the buyer are formalized and concluded under clear terms for their trading activities; (2) the seller and the buyer must indicate and agree on where the advertisement should (not) appear – they also have to establish mechanisms to minimize any misplacement (special software might have to be installed to that effect); (3) the seller has to confirm whether the measures apply and has to inform the buyer about the provisions that they apply in order to avoid any misplacement of the advertisement; (4) the seller explains its specific provisions in order to minimize the misplacement or its statement of reasonable endeavors – furthermore, the seller commits itself to inform the buyer about the process supporting the measures implemented; (5) if, however, those measures do fail and an advertisement has been misplaced, the seller and the buyer commit themselves to the contractual consequences that they have previously agreed on; (6) signatories must facilitate a procedure with the aim of reducing advertising misplacement approved by the Joint Industry Committee for Web Standards (JICWEBS) and verified by a verification provider[67].

F. FREEDOM OF EXPRESSION, COMPETITION AND DATA PROTECTION

42. While one of the main objectives of voluntary measures, codes of practice or other soft law mechanisms is to increase the effectiveness of IP rights enforcement online, it is important to strike a “fair balance” between the fundamental rights of the main actors involved in such

---

63 Ibid.

64 Austrian Ethics Code for the Advertising Industry (2014); UK principles of good practice of the trading of digital display advertising – EUIPO Study 2016, 14, 19–23. See WIPO/ACE/10/21 on Interactive Advertising Bureau (IAB) Poland’s initiatives. In EU similar practices have been initiated in Austria, Denmark, France, Italy, the Netherlands, Poland, Slovakia and the UK.

65 WIPO/ACE/10/21.

66 Ibid, 3.

67 EUIPO Study 2016. See also DTSG UK Good Practice Principles, (*JICWEBS*, 11 May 2017) http://www.jicwebs.org/digital-trading-standards-group-good-practice-principles/good-practice-principles accessed 16 July 2017.

procedures[68]. These fundamental rights include freedom of expression, lawful competition, privacy and data protection. In considering and balancing the underlying societal interests at stake, Professor Mel Nimmer's concept of "definitional balancing"[69] of opposing fundamental interests to arrive at an appropriate demarcation of boundaries is apposite here. As he aptly pointed out, virtually no right can be absolute – an absolutist starting point is both unrealistic and unreasonable. Rights have boundaries and their reach is limited by balancing opposing policies. Trademark rights must be balanced against freedom of expression, lawful competition and data-protection interests.

43. Trademark law can be misused by some rights holders to shut down competition from non-preferred resellers of genuine products and to control distribution channels[70]. For instance, if misapplied, "whitelists" where product listings or websites are approved by right holders could put at risk legitimate comparative advertising, sales of used, refurbished or genuine goods, and commentary on right holders[71]. Analogous concerns have been highlighted by Professor Bernt Hugenholtz in the copyright context, where intermediaries may adopt risk-adverse policies, removing legitimate listings and limiting freedom of expression and information[72]. Therefore, it is important that safeguards are in place to prevent misuse of trademark law to restrict lawful competition from non-preferred resellers of genuine products, and to control distribution channels. Safeguards could include penalties for misuse, counter-notice procedures and greater transparency. Any "whitelists" introduced must clearly be limited to serving solely as a reference point and checklist of authentic versus counterfeit for platforms, domain name registrars, law enforcement and administrative authorities to use as a source and provenance reference, and not to control distribution or interfere with the sale of genuine goods.

44. But like all such rights, freedom of expression, competition and data-protection rights also have their own limits if abused[73]. Professor Thomas McCarthy eloquently defines the underlying principles of trade mark law: "Trademark law serves to protect both consumers from deception and confusion over trade symbols and to protect the plaintiff's infringed trademark as property"[74].This tenet of trademark law also applies when a counterfeiter uses a trademark to deceive and lure web customers to their site through false pretenses and the use of another's registered trademark.

45. As a form of fraud, counterfeits raise no free speech issues. As the US Supreme Court and a number of other courts around the world have stipulated, deceptive speech is not protected speech[75]. Although there is an indisputable need to protect the privacy of individuals, there must also be an acknowledgement that the individuals and businesses that hide behind the rubric of privacy or free expression to conceal bad acts should not be allowed to continue.

---

[68] Knud Wallberg, "Notice and Takedown of Counterfeit Goods in the Digital Single Market: A Balancing of Fundamental Rights" [2017] *Journal of Intellectual Property Law & Practice*.

[69] Melville B. Nimmer, "Does Copyright Abridge the First Amendment Guarantees of Free Speech and Press?", *17 UCLA L. REV.* 1180 (1970), 1184–93.

[70] Chen (n 61).

[71] Ibid.

[72] Bernt Hugenholtz, "Code of Conduct and Copyright: Pragmatism v Principle", https://www.ivir.nl/publicaties/download/codes_of_conduct_and_copyright_pragmatism_v_principle.pdf accessed 3 August 2017.

[73] Frederick Mostert and Martin Scwhimmer, "Notice and Trackdown" (*Intellectual Property Magazine*, June 2011) 18–19.

[74] Thomas McCarthy, Trademarks And Unfair Competition § 2:2 (4th ed. 2014).

[75] Counterfeits as a form of deception qualifies as "deceptive speech" which the US Supreme Court has earmarked as unprotected speech under the First Amendment. See *Friedman v. Rogers*, 440 U.S. 1 (1979). See also Canadian Supreme Court in *R v Oakes* [1986] 1 S.C.R. 103 (finding that Canadian Charter of Rights and Freedoms that allows reasonable limitations on rights and freedoms through legislation if it can be demonstrably justified in a free and democratic society) and the European Commission on Human Rights in X and Church of Scientology [1979] 16 DR 68 at [79] (finding that misleading or deceptive commercial expression deserves the least protection).

As Justice Abella, along the same lines, cogently put it: "This is not an order to remove speech that, on its face, engages freedom of expression values, it is an order to de-index websites that are in violation of several court orders. We have not, to date, accepted that freedom of expression requires the facilitation of the unlawful sale of goods"[76].

IV. THE "RATIO" PRINCIPLES OF INTERMEDIARY RESPONSIBILITY – INTERNATIONAL COMMON APPROACHES

46. In general terms, although some jurisdictions may differ on certain aspects, it is found that liability for intermediaries falls into the following categories. First, the most basic is primary (or direct) infringement – doing the infringing act. Second, there is accessory (or secondary or contributory) liability – liability for assisting another person to do the infringing act. Both primary infringement and accessory liability expose the wrongdoer to an injunction and payment of damages. Third, there is intermediary liability. This exposes an intermediary to an injunction only, not damages. It does not require the intermediary to be either a primary infringer or an accessory. Primary infringement is generally strict liability, whereas both accessory liability and intermediary liability involve a mental element, usually some form of knowledge.

47. Although primary liability is in principle available, especially when the intermediaries use trademarks in their online advertising[77], online intermediaries typically only provide services which allow the online infringer to sell counterfeit products. Therefore, the law's response in most jurisdictions rests on the accessory liability of online intermediaries which have failed to meet the necessary "reasonable measures" when conducting their business of offering their services online[78].

48. It is of interest to note that throughout different jurisdictions in the world there are three key similarities between approaches to intermediary and accessory liability[79]. In effect, a "ratio" of common principles have emerged.

49. First, across all jurisdictions, intermediaries are not liable for accessory liability[80] if they had no knowledge of the specific infringement in question, subject to a finding of willful

---

[76] *Google Inc. v Equustek Solutions Inc.*, 2017 SCC 34 [42] (Abella J).

[77] In the US, liability based on s. 43(a) of the Lanham Act; Tiffany *v eBay* 600 F.3d 93 (2nd Cir. 2010) 113-114.

[78] Most jurisdictions justify secondary liability on common-law principles of tort or statutory tort law. In China Art. 36 of the Tort Law of the People's Republic of China – as reported in Ferrante, 257; in the US – developed from common law torts – *Tiffany v eBay* 600 F.3d 93 (2nd Cir. 2010), 103; in Republic of Korea the concept of "accessory liability" – explored in *Adidas*, Supreme Court Decision 2010Ma817, 4 December 2012, case note reported on WIL Map http://cyberlaw.stanford.edu/page/wilmap-south-korea. Similar principles of intermediary liability have been at play in the copyright context internationally. In Brazil – *Google Brazil v Dafra*, Special Appeal No. 1306157/SP (Superior Court of Justice, Fourth Panel, 24 March 2014); in Argentina – Rodriguez M. Belen c/Google y Otro s/ daños y perjuicios, R.522.XLIX. (Supreme Court, 29 October 2014); in Australia – *Roadshow Films Pty Ltd & Ors v iiNet Ltd* [2012] HCA 16; CCH *Canadian Ltd v. Law Society of Upper Canada* [2004] 1 SCR 339. By contrast, in Germany, liability is derived from a property law doctrine, the concept of *Störerhaftung*. As Kur explains: "This concept is derived by analogy from a provision in the civil code entitling proprietors to request that interferences resulting in detrimental effects on their property be removed and enjoined in the future . . . Objective liability standards apply, and guilt or negligence need not be established . . . Showing of detrimental effects is sufficient unless the interference must be tolerated by the proprietor for specific reasons" – A. Kur, 'Secondary Liability for Trademark Infringement on the Internet: The Situation in Germany and Throughout the EU' (2013–2014) 37 *Colum JL & Arts* 525, 532.

[79] Mostert and Asokan (n 8). Similarly, in the European context, Christina Angelopoulos has noted that while "the theoretical clashes between the European national systems might be considerable, in practice the results do not greatly differ. Structure, rather than substance is what diverges". *European Intermediary Liability in Copyright: A Tort-Based Analysis* (Kluwer Law International, 2016) 16–18.

[80] While different terms have been used to refer to this concept across jurisdictions, the substance remains the same. Other terms that have been used internationally include "contributory liability", "indirect liability", "secondary liability", "tertiary liability", "third party liability" and "interferer liability".

blindness[81]. Accessory liability is the liability of one person – the "accessory" – for their participation in an infringement committed by another – the "primary" or "principal" wrongdoer[82]. In other words, accessory liability is liability that is dependent on the prior liability of another party[83].

50. Second, an intermediary who fails to take measures expeditiously upon gaining specific knowledge of an infringement may lose its ability to enjoy safe-harbor protection from liability[84]. Generally speaking, safe-harbor provisions refer to rules which grant immunity to intermediaries from liability for damages under certain conditions. While the loss of safe-harbor protection will not result in an automatic finding of liability, the underlying principles of intermediary liability suggest such a finding may be likely in certain jurisdictions[85]. It is of interest to note that in virtually all jurisdictions safe harbors do not provide a defence to an injunction.

51. Third, there is increasing recognition of the availability of blocking injunctions against intermediaries or platforms – who while innocent of trademark infringement – must assist right holders in stopping and preventing further infringement. Website blocking orders are confined to taking proportionate measures and whether they are necessary and effective, among other requirements[86]. While it is unclear if there are substantive differences in the extent of preventative action required, there appears to be a common red line as no country currently imposes a general monitoring obligation on intermediaries. As a result, the scope of blocking injunctions is typically confined to taking preventative measures against the specific trademark violation identified by the right holder in the initial notice.

52. As has been noted[87], the three common tenets outlined above can be distilled into a transnational "ratio" principle of intermediary responsibility: *upon notice of a specific infringement, an internet service provider is required to take all proportionate and reasonable measures which a reasonable internet service provider would take in the same circumstances to address the specific instance of infringement brought to their attention*. The term "ratio" principle derives from Roman law. First, from the term *ratio decidendi* which refers to the core synthesis of a particular decision (usually by a court); in other words, the "reason" or "rationale" on which a decision is based. Second, the word for reasonable is *rationabile* in Latin. The "reasonable man" standard under a duty of care in common law is well known – as is the "bonus paterfamilias" principle in civil law systems, which equally relies on "reasonable" conduct under the same circumstances by the responsible party. Both these standards, and especially the term "reasonable", have surfaced frequently in discussions of online liability in a number of jurisdictions as a common thread[88].

---

81 *Tiffany v eBay* at 109-110. ("A service provider is not, we think, permitted willful blindness. When it has reason to suspect that users of its service are infringing a protected mark, it may not shield itself from learning of the particular infringing transactions by looking the other way..."). See also *Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.*, 658 F.3d 936 (9th Cir. 2011). at 1108.

82 Christina Angelopoulos, *European Intermediary Liability in Copyright: A Tort-Based Analysis* (Kluwer Law International, 2016) 16–18.

83 However, it does not necessarily follow that an intermediary who does have knowledge will be held liable as an accessory, as an additional component of intent or gross negligence is generally required for an intermediary to be held liable. Ibid 282-283.

84 This may vary depending on the nature of the intermediary. For instance, caching and mere conduit intermediaries might retain safe-harbor protection even if they do have knowledge of infringement.

85 For instance, the principles of joint tortfeasance in the UK or the application of art. 1383 and 1384 Code Civil in France.

86 See para 71 below.

87 Mostert and Asokan (n 8).

88 For instance, Christina Angelopoulos has adopted a similar approach in using the term "bonus medius interretialis" to refer to the reasonable intermediary. Christina Angelopoulos, *European Intermediary Liability in Copyright: A Tort-Based Analysis* (Kluwer Law International, 2016) 258.

53. This is an objective test analogous to the reasonable man test in common-law jurisprudence and the *bonus pater familias* standard in civil law. The value of recognizing this principle is clear: it provides a strong basis for a common core framework for intermediary liability internationally. Common standards are essential to facilitate cross-border enforcement which is vital in effectively addressing the challenge of counterfeiting in the borderless online environment. While formal harmonization of legal standards would be procedurally challenging, it is a suggested that this framework could take the form of a set of non-binding "voluntary guidelines" to facilitate the quick and efficient implementation among Member States in today's fast moving digital environment.

54. The word "reasonable" has surfaced in judgments around the world, providing greater clarity on the measures internet services providers must take to satisfy the "ratio" principle. A core guiding principle is striking an appropriate balance between the competing legitimate interests at play: the property interests of right holders in their trademarks, the freedom of internet service providers to conduct their business, the freedom of expression of internet users and intermediaries[89], and data protection and privacy interests[90]. As Graeme Dinwoodie points out, the need to balance these principles were identified in the European context by the CJEU's decision in Telekabel[91]. This reasoning also appears to underpin the judgment of Sullivan J in *Tiffany v eBay*, which held that eBay had implemented anti-counterfeiting measures as soon as it was "reasonably and technologically capable of doing so" against the claimant's assertion that eBay could have done more to prevent the sale of counterfeit goods on its platform. This suggests the concept of "reasonable" is not static, and the measures intermediaries should adapt can change over time.

55. In effect, this points to how the "ratio" principle is an inherently flexible standard that can be tailored to the specific parties in question. This is important as it allows the principle to account for platform differentiation. As Terri Chen points out, the diversity of platforms and ways trademarks are used on different platforms makes a one-size-fits-all approach inappropriate. For instance, a framework that is effective and appropriate in the context of commercial advertising networks or hosted e-commerce marketplaces might antagonize free-speech interests in relation to less commercially oriented products. Similarly, measures appropriate for a large, sophisticated internet service provider could likely differ from what might be appropriately imposed on one that is smaller provider with fewer resources. A series of judgments by Mr. Justice Arnold imposing blocking orders requiring internet service providers to block access to infringing websites in the United Kingdom demonstrates the virtues of adopting a flexible standard[92]. Mr. Justice Arnold has devised mechanisms to assuage concerns of both intermediaries and internet users on over-blocking, as well as right holders' concerns about the "whack-a-mole" problem[93]. For instance, he has enabled rights holders to "amend and augment blocking requests without having to initiate new, separate proceedings"[94], while also recognizing IP address blocking may be inappropriate where the relevant website's IP address is shared with other non-infringing users[95].

---

89 The freedom of expression of intermediaries was considered by the ECHR in *Delfi AS v. Estonia* ECtHR 64669/09, *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary*, ECtHR 22947/13 and *Pihl v. Sweden*, ECtHR 74742/14.

90 Data-protection rights were considered by the CJEU in Case C-70/10, *Scarlet Extended SA. v. Société belge des auteurs, compositeurs et éditeurs SCRL* (SABAM), C-360/10, *Sabam v. Netlog* and *Coty Germany GmbH v Parfümerie Akzente GmbH*, C-230/16. Privacy rights were considered in Case C‑275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*. This will certainly be relevant where the court is examining information disclosure orders.

91 Graeme Dinwoodie, *A Comparative Analysis of the Secondary Liability of Online Service Providers* 56–99 (Springer, Dinwoodie ed., 2017).

92 EU E-Commerce Directive Articles 12-15.

93 Ibid, 59–62. See also WIPO/ACE/12/19, pp. 22-26.

94 Ibid, 62. See also Mostert and Asokan (n 8).

95 *Dramatico Entertainment Ltd. v British Sky Broadcasting Ltd*. [2012] EWHC 1152 (Ch), [13] (Arnold J).

A. WHAT IS THE LEGAL STANDARD FOR QUALIFYING AS AN INTERMEDIARY?

56. The legal standard for qualifying as an intermediary has been the subject of a fair amount of discussion with policymakers and in legal circles. A common view holds that intermediaries refer to "entities that facilitate in any way the use of the internet by others to access content produced by third parties. It is suggested that three basic conditions can be identified. The actor must: (a) provide services related to the internet; that (b) involve content produced by somebody else; and (c) are used by third parties"[96]. As Christina Angelopoulos points out, it is the go-between nature of internet intermediaries that makes them particularly susceptible to accessory liability: "internet intermediaries are essentially accessories to all conduct of all third parties that use their services. When that conduct illegally impacts somebody else, the spectre of liability looms"[97].

B. DEFENCES

57. Some jurisdictions provide for "safe-harbor" exemptions from liability. The conditions required to enjoy safe-harbor exemptions vary according to the nature of the intermediary. For example, in the European Union, the mere conduit and caching safe harbors require that the provider does not contribute to the content creation, and the exemption applies even with knowledge of infringement. However, for hosting safe-harbor exemptions to apply, the host cannot have knowledge of specific infringement. Safe-harbor provisions also vary between jurisdictions[98]. While the safe-harbor provisions in the United States and European Union are similar, Canadian law has adopted notice-and-notice system[99] while Japanese law uses a notice-wait-and-take-down system[100].

C. ACCESSORY LIABILITY

58. Where safe harbor or other defenses do not apply, intermediaries may be held liable either directly or as an accessory for infringement. To escape liability, online intermediaries are bound by a "standard of behavior". Attempts to define this standard on behalf of the intermediaries is not yet clear or uniform. Equally, it is unclear what are the preventative actions to be taken by an intermediary once a specific infringement has been notified by the rights holder.

59. In China, for example, the standard of intermediary "indirect" liability is one of "reasonable care"[101]. Under Art. 36 of Tort Law, service providers must take necessary measures after they have been informed of infringing content, and failing to do so will result in their "joint and several" liability with the user. Service providers' knowledge of the infringing behavior can thus result in liability with the user, unless the service provider reacts to notice by taking

---

[96] Christina Angelopoulos, *European Intermediary Liability in Copyright: A Tort-Based Analysis* (Kluwer Law International, 2016) 11. See also B. Martinet Farano, "Internet Intermediaries' Liability for Copyright and Trademark Infringement: Reconciling the EU and US Approaches" (2012) TTLF Working Paper No. 14, 100.

[97] Ibid.

[98] See generally Zingales, Nicolo, "Internet Intermediary Liability: Identifying Best Practices for Africa" (25 November 2013). Intermediary Liability in Africa Research Series, Association for Progressive Communications, forthcoming. Available at SSRN: https://ssrn.com/abstract=2359696. In China, safe-harbor provisions are provided in Article 23 Chinese Internet Regulation.

[99] Government of Canada Office of Consumer Affairs, "Notice and Notice Regime" (17 June 2014) https://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca02920.html accessed 1 August 2017.

[100] Christina Angelopoulos and Stijn Smet, "Notice-and-Fair-Balance: How to Reach a Compromise between Fundamental Rights in European Intermediary Liability" (2016) 8 *Journal of Media Law* 266, 296–297.

[101] Article 36 of Tort Law of the People's Republic of China.

countermeasures[102]. Since 2011, courts have established that the standard of reasonable care, which excuses the service provider from indirect liability, requires more than simply compliance with a "notice and take-down" procedure. Service providers must take more stringent measures to end unlawful activities, such as, "publicly condemning the online seller's unlawful activities; downgrading the seller's 'trustworthiness rating' (information available on the website); limiting the use of the website (by prohibiting the seller from selling certain products) and[103], as a last resort, banning the online seller from using the online platform"[104].

60. The shift seen in Chinese courts was also accompanied by further policy measures. The Circular of the Ministry of Commerce imposed several duties on the online intermediaries and e-commerce operators, including the duties to "(i) establish a trade mark and patent inquiry system; (ii) adopt technical measures to monitor IPR infringements; (iii) improve accessibility to information on sellers, payments details, logistics, after-sale service, dispute resolution, compensation, process monitoring; (iv) institute a daily online inspection system; (v) investigate and remove infringing content in a timely manner; (vi) handle violations of regulations and laws; and (vii) report serious cases to the competent authorities in a timely manner"[105]. These measures were reiterated in the Administrative Measures for Online Trading by the State Administration for Industry and Commerce in 2014[106].

61. In the Republic of Korea, "open-market" operators' accessory liability is based on previous knowledge of a specific infringement and the possibility of taking preventative measures. Whereas there is no general obligation to monitor content online, once a notice of infringement has been given, the intermediary is under the duty to prevent further listings of the same infringing products[107].

62. In the United States, contributory trademark infringement was highlighted in the *Tiffany v eBay* decision, which applied the "know or has reasons to know" of the infringement test (the *Inwood* test)[108.] There are two ways in which liability of service providers may be established under *Inwood*: first, if the service provider "intentionally induces another to infringe a trademark", and second, if the service provider "continues to supply its [service] to one whom it knows or has reason to know is engaging in trademark infringement"[109].

---

[102] Ferrante, 257.

[103] Ferrante, 258 (*E-Land International Fashion (Shanghai) Co., Ltd. v Du Guofa and Zhejiang Taobao Internet Co., Ltd*, Case No. 40, First Intermediate People's Court of Shanghai, 25 April 2011).

[104] Ferrante, 258 (referring to C. Jianmin "Case Comment: *Yinian (Shanghai) Garments Trading Co., LTD.* v *Zhejiang Taobao Network Co., LTD. and Du Guofa*" (2011–12) 4 *Tsinghua China L Rev* 283, 287).

[105] M. Ferrante, "E-commerce platforms: liability for trade mark infringement reflections on Chinese courts' practice and remedies against the sale of counterfeits on the internet" (2015) 10(4) *JIPPL* 255, 258–259 (*E-Land International Fashion (Shanghai) Co., Ltd. v Du Guofa and Zhejiang Taobao Internet Co., Ltd*, Case No. 40, First Intermediate People's Court of Shanghai, 25 April 2011; referring to C. Jianmin "Case Comment: *Yinian (Shanghai) Garments Trading Co., LTD. v Zhejiang Taobao Network Co., LTD. and Du Guof*" (2011–12) 4 *Tsinghua China L Rev* 283, 287; providing the English translation for "Circular of Further Pushing Forward the Crackdown on Intellectual Property Right Infringement and Manufacturing and Sale of Passing-offs and Inferior Products in the Online Shopping Sector" and Administrative Measures for Online Trading (State Administration for Industry and Commerce, 2014)).

[106] Ibid.

[107] *Adidas*, Supreme Court Decision 2010Ma817, 4 December 2012, a case note available on WIL Map http://cyberlaw.stanford.edu/page/wilmap-south-korea.

[108] *Tiffany v eBay* 104–105 ("the Ninth Circuit concluded that Inwood's test for contributory trademark infringement applies to a service provider if he or she exercises sufficient control over the infringing conduct. *Lockheed Martin Corp. v. Network Solutions, Inc*., 194 F.3d 980, 984 (9th Cir.1999)); *Inwood Laboratories, Inc. v. Ives Laboratories, Inc.*, 456 U.S. 844, 102 S. Ct. 2182, 72 L.Ed.2d 606 (1982) (test for contributory trademark infringement).

[109] *Tiffany v eBay* 600 F.3d 93 (2nd Cir. 2010) 104–106; Inwood *Laboratories, Inc. v. Ives Laboratories, Inc.*, 456 U.S. 844 (1982).

63. As to the first situation, the conduct of the intermediary is relevant – an intermediary will not be liable, if it applies reasonable anti-counterfeiting measures[110]. As to the second situation, general knowledge is not sufficient; what is required is knowledge of specific instances of infringement[111]. The threshold of "knowledge" is high and a claim of contributory trademark infringement would only succeed if there is "[s]ome contemporary knowledge of which particular listings are infringing or will infringe in the future"[112].

64. It should be noted that so far "willful blindness" is not a separate ground for establishing liability. As the court noted, if eBay was aware of, or turning a blind eye to, specific infringers, *Inwood* liability would arise[113]. General knowledge of some counterfeit sales occurring in its online market place cannot be equated with "wilful blindness".

65. In the European Union, safe-harbor exemptions cover all liability from IP infringement by virtue of the E-Commerce Directive[114].

D. DUTY OF CARE

66. There have been some suggestions that duty of care be defined as the appropriate legal standard of liability for intermediaries[115]. A potential advantage of this approach to intermediary and accessory responsibility would be to make it easier to impose liability on intermediaries that do not intend third party infringement, but carelessly occasion them[116].

67. However, as Davies points out in relation to intermediary liability, "It might finally be noted that it is unlikely that an accessory could be liable in negligence, as it is difficult to establish that such an accessory owes any duty of care to the claimant. [... It] seems inappropriate for negligence to trespass upon an area which is already regulated by principles of accessory liability"[117].

---

110 *Tiffany v eBay* 104-106 ("The district court concluded that "eBay consistently took steps to improve its technology and develop anti-fraud measures as such measures became technologically feasible and reasonably available.")*Tiffany v eBay* 99 ("For nearly a decade, including the period at issue, eBay has also maintained and administered the 'Verified Rights Owner (VeRO) Program'" - a "'notice-and-takedown' system" allowing owners of IP rights, including Tiffany, to ''report to eBay any listing offering potentially infringing items, so that eBay could remove such reported listings". Any such right holder with a ''good-faith belief that [a particular listed] item infringed on a copyright or a trademark'' could report the item to eBay, using a ''Notice of Claimed Infringement form or NOCI form''), 100 (the Court found that eBay reacted to all specific notices of trademark infringement by removing the infringing listings (the NOCI procedure)).

111 *Tiffany v eBay* 108 (referring to *Sony Corp. of America v. Universal City Studios, Inc*., 464 U.S. 417, 104 S.Ct. 774, 78 L.Ed.2d 574 (1984) (Sony's liability as the manufacturer and seller of video recorders - reading of *Inwood* must be narrow, so that the defendant must know the identity of the infringers).

112 *Tiffany v eBay* 107.

113 "In the words of the Seventh Circuit, ''willful blindness is equivalent to actual knowledge for purposes of the Lanham Act.'' Hard Rock Café, 955 F.2d at 1149." *Tiffany v eBay* 108.

114 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 (E-Commerce Directive), Articles 12–15.

115 C McIvor, *Third Party Liability in Tort* (Hart Publishing 2006) 50-65. See also C McIvor, "Liability for the Acts of Third Parties: Tort Lessons for Intermediary Copyright Liability", roundtable discussion on "The European Harmonisation of Intermediary Accessory Liability for Online Copyright Infringement: at the Intersection of Tort Law and Fundamental Rights", 13 April 2015, Institute for Information Law (IViR), Amsterdam.

116 Christina Angelopoulos, *European Intermediary Liability in Copyright: A Tort-Based Analysis*, (Kluwer Law International, 2016) 121.

117 P S Davies, "Accessory Liability: Protecting Intellectual Property Rights" (2011) *4 Intellectual Property Quarterly* 390.

E. INJUNCTIONS

a) Injunctions for blocking websites by internet service providers

68. Some jurisdictions have now recognized the possibility of issuing an injunction against an ISP (a blocking injunction), who although innocent of trademark infringement must assist the trademark owner in stopping and preventing further infringement. The most notable developments have recently been seen in the UK[118]. Outside Europe, both Australia[119] and Singapore[120] have passed legislation to facilitate website blocking; however, this has only been applied in the copyright context thus far[121].

69. In the UK, there is no specific legislative provision stipulating for the issuing of blocking orders in the case of trademark infringement. Although there is no statutory provision like s. 97(A) CPDA for copyright, courts have found power to issue blocking orders in online trademark counterfeit cases based on the broad powers of s. 37 of the Senior Courts Act 1981[122], in line with the United Kingdom's obligation under Article 11 of the Enforcement Directive to provide such injunctions. This was established in the case of *Cartier*, which has been confirmed by the Court of Appeal[123]. Courts' discretion to issue a blocking injunction against an ISP on the basis that services were being used to infringe a trademark is based on four conditions[124]: (1) the ISP is an "intermediary" within the meaning of Art. 11 of the Enforcement Directive[125]; (2) the users and/or the operators of the website are infringing the claimant's trademark; (3) the users and/or the operators of the website are using the ISP's services to do so; (4) the ISP had actual knowledge of this.

70. Per Article 3 of the Enforcement Directive, website blocking injunctions must be[126]: (1) necessary (to be tested through the principle of proportionality); (2) effective[127]; (3) issuasive[128]; (4) not unnecessarily complicated or costly[129]; (5) must avoid the creation of

---

118 See "Website Blocking Injunctions: The UK Experience" in WIPO/ACE/12/10.

119 Copyright Amendment (Online Infringement) (Australia) Act 2015.

120 Copyright Amendment (Singapore) Act 2014.

121 *Roadshow Films Pty Ltd v Telstra Corporation Ltd* [2016] FCA 1503. See also Andy Leck and Faith Lim Yuan, 'Updates on Site Blocking' (*Lexology*, 7 February 2017) http://www.lexology.com/library/detail.aspx?g=fdd9555c-8c11-44b0-b3e9-514165652778 accessed 1 April 2017.

122 No specific implementation of Arts 3 and 11 of the Enforcement Directive needed; this broad discretion can be exercised in online trade mark counterfeit cases – CA in *Cartier International AG and others v British Sky Broadcasting Ltd and others (Open Rights Group intervening)* (CA 6 July 2016) [2016] EWCA Civ 658, [2017] Bus. L.R. 1 [72].

123 *Cartier* – Dismissing all appeals and affirming the Decision of Arnold J [2014] EWHC 3354 (Ch); [2015] Bus LR 298; [2015] 1 All ER 949; [2015] 1 All ER (Comm) 641; and the Decision of Arnold J [2014] EWHC 3915 (Ch); [2015] 1 All ER 1027; [2015] 1 All ER (Comm) 718; and Decision of Arnold J [2014] EWHC 3794 (Ch).

124 CA in *Cartier* [80].

125 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).

126 Art. 3(2) of the Enforcement Directive.

127 Aimed at defendant. Overall on efficiency, Arnold J relied on the blocking injunctions in copyright cases and found that "blocking of targeted websites has proved reasonably effective in reducing use of those websites in the UK. No doubt it is the casual, inexperienced or lazy users who stop visiting those websites, whereas the experienced and determined users circumvent the blocking measures; but that does not mean that it is not a worthwhile outcome" – CA in *Cartier* [179] (agreeing with Arnold J [236]).

128 Aimed at third parties CA in *Cartier* [119].

129 Applying Art. 3(1) Enforcement Directive and interpretation in CJEU *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (Judgment, 24 November 2011) Case C-70/10, ECLI:EU:C:2011:771, [48] and *UPC* [50] – costs can be borne by the intermediary, but they cannot be unnecessarily complicated or costly – all of which is an assessment of proportionality – CA in *Cartier* [122]; [157] (costs and benefits are to be assessed carefully on the evidence (including the ranking (i.e. popularity – per Alexa Ranking) of target websites).

barriers to legitimate trade[130]; (6) be fair and equitable[131]; and (7) strike a "fair balance" between the applicable fundamental rights and be proportionate[132]. Finally, it is necessary to consider the substitutability of other websites for the target websites and the requirement in article 3(2) of the Enforcement Directive that remedies should be applied in such a manner as to provide safeguards against their abuse[133].

71. In principle, IP address blocking can be proportionate, if the right procedure is followed[134]. The court took the following circumstances into consideration in its proportionality analysis[135]: (1) the comparative importance of the rights that were engaged and the justifications for interfering with those rights; (2) the availability of alternative measures which were less onerous; (3) the efficacy of the measures that the order required the ISPs to adopt, and in particular whether they would seriously discourage the ISPs' subscribers from accessing the target websites; (4) the costs associated with those measures, and in particular the costs of implementing the measures; (5) the dissuasiveness of those measures; (6) the impact of those measures on lawful users of the internet; and (7) the substitutability of other websites for the target websites.

b) Injunctions for removing content on online platforms

72. In some jurisdictions establishing trademark infringement on the side of an online intermediary is difficult, particularly in cases of sales of online counterfeits, because the intermediaries do not "use a trademark" either in "the course of trade" or "as a trademark".

73. In response to this challenge, some jurisdictions have recognized the availability of blocking injunctions such platforms. In Germany, this approach is based on the "*Störerhaftung*" doctrine. As Christina Angelopoulos notes, *Störerhaftung* functions as a form of strict liability limited to injunctive relief. The doctrine establishes tortious liability for IP infringement under the following conditions: (1) the defendant is not liable for either primary or secondary IP infringement; (2) there must be an adequate causal link between the acts or omissions of the defendant and the IP infringement (can be ongoing) and this results in "interference"; and (3) the defendant must have the means (factual or legal) to remove the cause of the ongoing infringement[136].

74. Specifically, in the online context, the *Störerhaftung* doctrine was developed in the "internet auction" cases[137]. In this context it was established that platform providers in online markets are not liable for trademark infringement unless they had actual knowledge of the infringement. Once made aware of the infringement, intermediaries can be held liable as an

---

130 Requirement in Art. 3(2) Enforcement directive means that "requires the measures adopted by the ISP to be strictly targeted so that they do not affect users who are using the ISPs' services in order lawfully to access information". *Cartier* [123].

131 Requirement from Art. 3(1) Enforcement Directive will be met, if measures are proportionate.

132 CA in *Cartier* [100].

133 CA in *Cartier* [101].

134 Non infringing sites must have the opportunity to be moved to other servers – CA in *Cartier* [77]–[78].

135 CA in *Cartier* [127].

136 Kur, 532, 533 (there will be no liability, if there was no incurring duty to monitor, which was disregarded).

137 Kur, 535 at fn. 61 referring to: Bundesgerichtshof [BGH] [Federal Court of Justice] Apr. 30, 2008, Gewerblicher Rechtsschutz und Urheberrecht [GRUR] 702, 2008 (Ger.) (Internet Auction III); Bundesgerichtshof [BGH] [Federal Court of Justice] 19 April 2007, Gewerblicher Rechtsschutz und Urheberrecht [GRUR] 708, 2007 (Ger.) (Internet Auction II); Bundesgerichtshof [BGH] [Federal Court of Justice] Mar. 11, 2004, 36 *Int'l Rev. of Intell. Prop. & Competition L.* 573, 2005 (Ger.) (Internet Auction 1). All three cases are extensively explored in *L'Oreal SA v. eBay International AG*, [2009] EWHC (Ch) 1094, [455] (Arnold, J).

"interferer" and injunctive relief granted and preventative measures ordered[138]. It is important to note that as part of the German *Kerntheorie* in *Störerhaftung*, actual knowledge is viewed as extending to all easily recognizable future unlawful acts of an essentially similar nature to the one that was notified.

c) How effective are blocking injunctions from a technical IT perspective?[139]

75. It should be noted that internet users can employ techniques to deliberately circumvent blocking injunctions, potentially undermining its effectiveness. Blocking injunctions require to block access to websites that host or facilitate access to infringing content. While a blocking injunction does not remove the infringing website from the internet, internet users who access the internet through ISPs who have instituted the block will not be able to access the website.

76. While results have been mixed, some studies suggest circumventing website blocking injunctions could appear to be easy. One of the most notorious infringing websites, The Pirate Bay ("TPB"), was blocked in the United Kingdom in 2012. Yet, in 2017, simply searching for the "The Pirate Bay" on Google from within the United Kingdom immediately yields a link to a list of duplicate, "mirror" TPB websites as the very first result (see Figures 1–2 below), enabling the block to be bypassed without any technological intervention on behalf of a user. This apparent ease of circumvention is congruent with the initial findings by Danaher, Smith and Telang which found that the 2012 blocking of TPB in the United Kingdom led to a minimal decrease in overall levels of piracy, and no impact on rates of legal streaming as users circumvented the block or turned to alternative sources[140]. A similar block on TPB instituted in the Netherlands yielded similar results, with Poort et al. finding only a small reduction in piracy[141].

77. A more sophisticated means of circumventing blocking orders can be accomplished by use of a virtual private network ("VPN"). VPNs enable an internet user to establish a secure and encrypted connection to a separate server through which web traffic is funnelled. Provided the VPN server to which a user is connected is outside of the jurisdiction in which a blocking order is active, the user would be able to connect to, and interact with, a blocked website. For example, if a Virgin broadband subscriber in London was prevented via a blocking order from accessing a website known to trade in counterfeits, the user would simply activate a VPN that tunnels web traffic through France, then back to the United Kingdom, and because the traffic is encrypted en route, Virgin would have no knowledge that the technical means it had implemented to give effect to a blocking order was being obviated. Crucially, legislation such as the UK Investigatory Powers Act ("UK IP Act"), which many internet users see as antithetical to

---

138 Kur, 535. In copyright context specific monitoring duties were imposed on RapidShare, an online digital storage provider in cases of "Alone in the Dark" (Bundesgerichtshof [BGH] [Federal Court of Justice] 12 July 2012, Gewerblicher Rechtsschutz und Urheberrecht [GRUR] 370, 2013 (Get.) (the case involved illegal distribution of a video game through the cloud administered by RapidShare)) and "File Hosting Dienst" Bundesgerichtshof [BGH] [Federal Court of Justice] 15 August 2013, Gewerblicher Rechtsschutz und Urheberrecht [GRUR] 1030, 2013 (Get.) (File-Hosting-Dienst) – discussed in Kur, 538, 539 (at fn. 92 finding that courts in these cases imposed the duty to "investigate, through search engines such as Google, Facebook or Twitter using appropriately formulated searches and possibly also with the assistance of so-called webcrawlers, whether indications can be found as to further illegal links to its service with regard to the relevant works"), 540 (although possible, these monitoring duties not yet applied in trademark context).

139 This section draws heavily on Asokan's review of existing measures address online copyright infringement – Sabesh Asokan, 'Online Copyright Infringement: A De Novo Review of the Existing Approach' (undergraduate dissertation, King's College London, 2017).

140 Brett Danaher, Michael D. Smith and Rahul Telang, "The Effect of Piracy Website Blocking on Consumer Behavior" (2015) *Carnegie Mellon University Working Paper* http://ssrn.com/abstract=2612063 accessed 1 April 2017. See also WIPO/ACE/10/20, "Copyright Enforcement in the Digital Age: Empirical Economic Evidence and Conclusions".

141 Joost Poort and others, "Baywatch: Two Approaches to Measure the Effects of Blocking Access to The Pirate Bay" (2014) 38 *Telecommunications Policy* 383.

privacy rights, has encouraged more widespread use of VPNs for ordinary web-browsing activity because it would prevent an intermediary such as Virgin from retaining any meaningful data about a user's web browsing activity, as mandated by the UK IP Act.

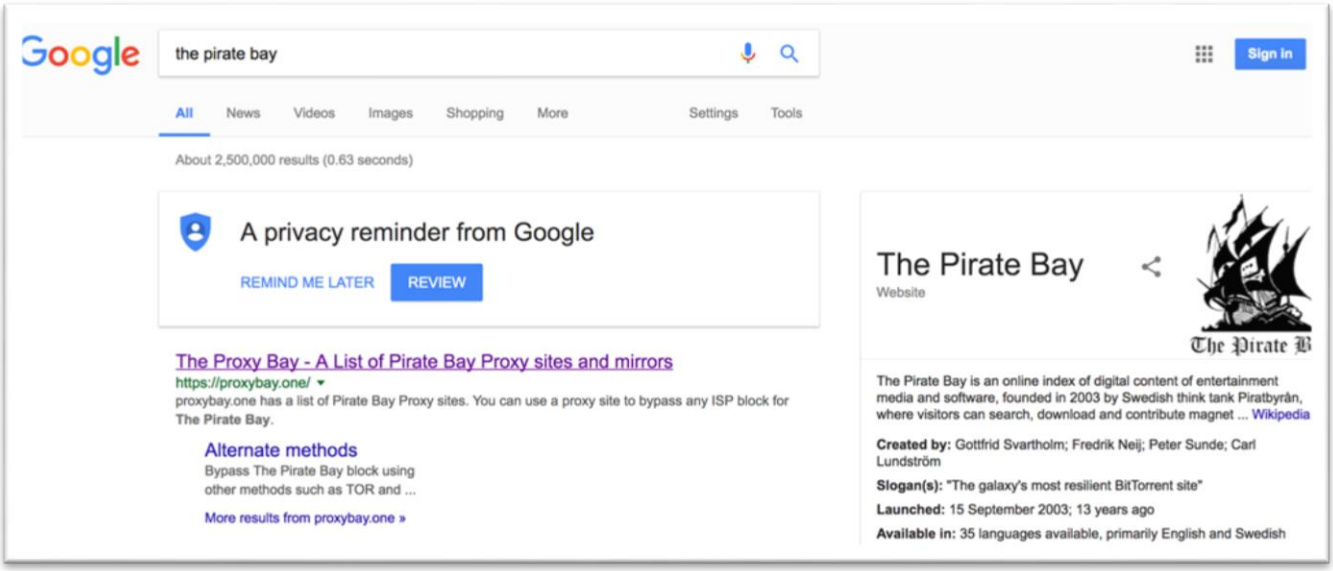

Figure 1: Screenshot of Google Search for "The Pirate Bay", 29/04/2017. The TPB slogan displayed prominently on the right pane appears unfortunately apt.

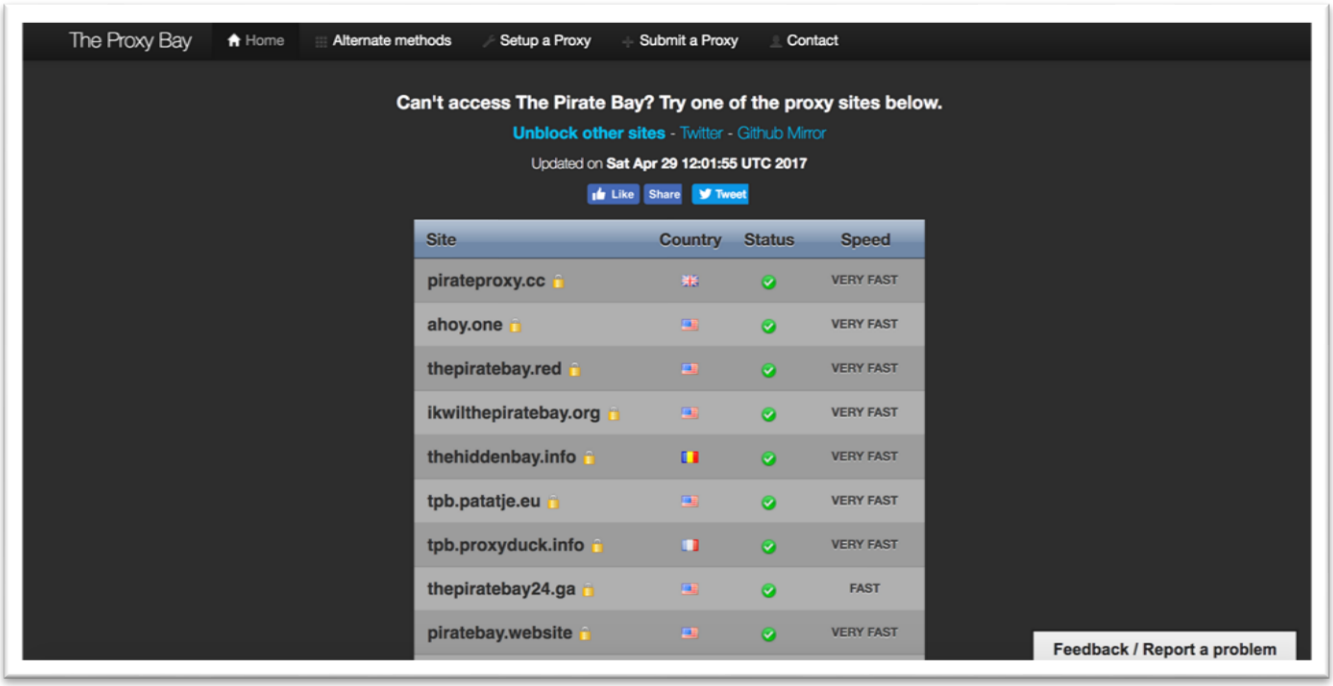

Figure 2: Screenshot of "The Proxy Bay", 29/04/2017. This website allows users to bypass the TPB blocking injunction without any technical intervention.

78. However, subsequent evidence reveals that website blocking orders are effective at reducing online copyright infringement when they are applied to multiple popular sources of infringing content simultaneously. A study found that the blocking of 53 key infringing websites in 2014 led to a 16 per cent decrease in overall piracy levels alongside a 6 per cent increase to

sources of paid legal content such streaming websites like Netflix, and ad-supported sources of legal content such as BBC and Channel 5's streaming portals[142]. In addition, unlike the initial block of TPB in 2012, the study did not find a concomitant causal shift to infringing websites that remain unblocked[143].

79. Consequently, the results suggest when website blocking orders are applied comprehensively, they are able to effectively deter casual potential infringers by raising the transaction and search costs associated with finding alternative sources of infringing content[144]. This is aligned with the notion that perceived benefits are an important driver of infringement as survey evidence suggests that individuals perceive that convenient access to content is a key benefit of online infringement[145]. While determined or technologically sophisticated internet users may be able to circumvent website blocks[146], these users are, at the moment, fewer in number, and their continued infringement does not fundamentally undermine the overall efficacy of the measure.

80. Yet, as the simple Google search for TPB above has underscored, the efficacy of supply-side measures depends on right holders' continual vigilance in ensuring blocks are imposed on alternative "mirrors" or sources of infringing content which emerge. This continual burden entails significant costs for right holders, which could potentially increase in the future as the legal position on who bears the costs of an injunction is not settled[147].

F. THE CRUCIAL COST FACTOR: WHO SHOULD BEAR THE COST OF POLICING AND STOPPING THE SALES OF ONLINE COUNTERFEITS?

81. As Stacey Dogan pointed out, both the courts and the legislature have adopted a modified "best-cost-avoider" approach in the US. This requires the burden of the costs to be shared between right holders and intermediaries, with the party best suited to carrying out a task responsible for its attendant costs. In practice, this means that the costs and responsibility for "detection falls on the intellectual property owner, who is best suited to recognize unauthorized versions of its work or trademark" while "responsibility for terminating the infringement, in turn, rests on the intermediary, assuming that it has specific knowledge and control over the means used to infringe"[148].

82. In the European Union, there has been no explicit recognition of the "best-cost-avoider" principle[149]. The courts have held that the cost of implementing blocking injunctions currently rests with the ISPs[150] and not the right holder. In certain cases[151], these costs can be imposed

---

142 Brett Danaher, Michael D. Smith and Rahul Telang, "Website Blocking Revisited: The Effect of the UK November 2014 Blocks on Consumer Behavior" (2016) Carnegie Mellon University Working Paper https://ssrn.com/abstract=2766795 accessed 1 April 2017.

143 Ibid., 13–14.

144 Ibid.

145 European Union Intellectual Property Office (n. 9) 14.

146 Danaher, Smith and Telang (n. 94) 11–12.

147 Eleonora Rosati, "Intermediary IP Injunctions in the EU and UK Experiences: When Less (Harmonization) is More?" GRUR International (forthcoming) <https://ssrn.com/abstract=2891042> accessed 1 April 2017, 11–20.

148 Stacey L. Dogan, "Principled Standards vs. Boundless Discretion: A Tale of Two Approaches to Intermediary Trademark Liability Online", 37 *Colum. J.L. & Arts* 503, 509–510 (2014).

149 In the context of copyright, Recital 59 of the InfoSoc Directive does recognize that intermediaries are best placed to bring infringing activities to an end. However, while intermediaries may be "best placed" to stop infringement, it does not follow that they should bear the cost of doing so.

150 Majority of CA in *Cartier* [145], [150] (Kitchin LJ and Jackson LJ), agreeing with Arnold J, who justified his decision by referring to his decision in *Twentieth Century Fox Film Corpn v British Telecommunications plc* (second judgment) [2012] Bus LR 1471, [53] (copyright) and CJEU in *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH* [2014] Bus LR 541, [50].

151 The principle of proportionality must be applied – CA in *Cartier* [163].

on the right holder, but this was not the case in the leading case of *Cartier*[152]. It is interesting to note the absolute numbers. In *Cartier*, estimates by ISPs of the costs of implementing the blocking injunction generally ranged from a "low four figure sum" to a "low five figure sum" while one ISP estimated it would cost "low six figure sum"[153]. Most recently, in France, the Cour de Cassation has held that ISPs can be ordered to pay all the costs of blocking injunctions and filtering injunctions, even where their liability is not engaged[154].

83. However, this issue has not been settled definitively[155]. In the United Kingdom, Lord Justice Briggs in the Court of Appeal in *Cartier* dissented and held that the cost of implementation for a particular blocking order should always fall upon the right holder making the application for it[156]. This is currently a live issue, pending appeal to the Supreme Court[157]. Adopting Briggs LJ's approach would entail a shift to the current Australian position outlined in *Roadshow Films v Telstra Corporation*, where Nicholas J held that that right holders "should be required to pay the respondents' compliance costs or some significant proportion thereof"[158]. Here, "compliance costs" refer to the same "implementation costs" Briggs LJ identified in *Cartier*.

84. Given the territorial nature of website blocking injunctions, the issue of costs is exacerbated in the cross-border context[159]. This is because it may be necessary for right holders to pursue and bear the costs of blocking injunctions in multiple jurisdictions to make a meaningful reduction in overall infringement levels given the global nature of the online environment.

85. Consequently, while effective, the cost of website blocking orders can put it out of the reach of many right holders. For instance, a recent public consultation by the European Commission on the effectiveness of existing enforcement procedures noted that cost and procedural length were the two key reasons why right holders failed to apply for website blocking injunctions[160]. This is especially true in the context of small and medium-sized enterprises (SMEs). As noted in the European Union Intellectual Property Office SME Scoreboard 2016, 58 per cent of SMEs refrain from employing legal procedures to enforce their intellectual property rights due to costs[161].

---

152 CA in *Cartier* [149] (as Arnold J in his decision in *Twentieth Century Fox Film Corpn v British Telecommunications* [53]).

153 *Cartier* [19] (Kitchin LJ).

154 Cour Cass, Civ 1, 6 July 2017, *SFR and others v Association of cinema producers and others*, No 16-17.217, 16-18.298, 16-18.348, 16-18.595, ECLI:FR:CCASS:2017:C100909.

155 Sabesh Asokan, "Online Copyright Infringement: A De Novo Review of the Existing Approach" (undergraduate dissertation, King's College London, 2017) 20–21.

156 Briggs LJ in *Cartier* [198], [211] (reasoning based on pre-existing case law on injunctions issued against innocent third parties, who got "mixed up" in the wrongdoing of a third party *Norwich Pharmacal Co* [1974] AC 133 by Lord Reid (in relation to the duty to assist the victim of a tort). And applied by the Court of Appeal in *Bankers Trust Co v Shapira* [1980] 1 WLR 1274 (orders to banks to disclose confidential information about their customers).

157 Elenora Rosati, "The Next Round of Cartier: UK Supreme Court Will Hear Appeal re Costs of Intermediary Injunctions" (*The IPKat*, 4 February 2017) https://ipkitten.blogspot.co.uk/2017/02/the-next-round-of-cartier-uk-supreme.html accessed 1 April 2017.

158 *Roadshow Films Pty Ltd v Telstra Corporation Ltd* [2016] FCA 1503 [147] (Nicholas J).

159 Asokan (n 147) 21–22.

160 *European Commission*, "Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, Public consultation on the evaluation and modernization of the legal framework for the enforcement of intellectual property rights – Summary of responses" (2016) 33.

161 EUIPO, *IP SME Scoreboard 2016,* 23.

86. Therefore, as Graeme Dinwoodie prudently states, the issue of who should bear the cost ought best be handled in a context-specific manner, sensitive to the particular factual matrix and competing principles at play[162]. For instance, the costs of identifying counterfeit articles may differ between parties and this would affect how the competing interests at play should be balanced[163]. Thus, if file-matching technology employed by intermediaries is most cost-efficient in identifying counterfeit material, the costs of identifying infringers might be better borne by intermediaries than right holders who may have to rely on labor and cost-intensive manual detection. Similarly, as intermediaries such as Alibaba adopt new technologies such as optical character recognition to detect counterfeits more cheaply and at a lower cost[164], this could weigh on the calculus on who is best placed to bear the costs of identifying counterfeits. Moreover, the position on costs may differ depending on the IP right involved as "the range of permissible uses may vary between copyright and trademark, altering the calculus of effect on the conduct of legitimate business"[165].

87. In a nutshell, right holders are typically the only parties capable of identifying whether a given product is counterfeit as Terri Chen[166] and Jay Monahan[167] accurately point out, while only intermediaries can remove counterfeit listings from their platforms.

88. In summary, on the crucial point of costs, as noted in the Financial Times: "Where do the recent epic legal battles leave web customers who are saddled with counterfeits daily? That there is a plethora of fakes online is glaringly obvious. Who then is responsible for removing the counterfeit products listed on (platforms). As in so many walks of life, the answer lies in the constructive co-operation. The answer for assessing responsibility lies in the middle – both sides should in equal measure diligently confront the online counterfeit problem together. Brand owners and auction sites need to work together and share the responsibility to stop fakes, like wildfire, to avoid a restraint on the progress of society."[168]

89. History repeats itself. The current cost issues and conflict between platforms and brand owners are similar to the concerns voiced when the first railways were constructed in the 1800's - in the interest of society's infrastructure. The legal question raised back then: if a spark from a steam locomotive flew on to crop and set them ablaze: who bore the loss – the railway company or the farmer? In the end reason prevailed – progress could not be halted if railway companies were subject to a flood of legal claims. However, the poor farmer could not be left carrying the full weight of the damaging consequences of scientific innovation. The solution: railway companies and farmers agreed to a voluntary middle ground: firebreaks along the tracks and spark arresters on the trains to minimize or prevent the harm[169].

90. Consequently, in the interest of the advancement of society in creating a world-wide cyber infrastructure, the implicit fact is that neither right holders nor intermediaries can avoid this new and burdensome responsibility. Brand owners will have to be the primary source of information for whether something is counterfeit because no-one else can do this. And equally, intermediaries will have to take more responsibility for what is on their sites, because no-one else can do this. So both "sides" have to accept the new reality that they both have new costly burdens to undertaken in the interest of society. On the basis that an injunction is an equitable

---

162 Graeme Dinwoodie, *A Comparative Analysis of the Secondary Liability of Online Service Providers* 71 (Springer, Dinwoodie ed., 2017).

163 Ibid.

164 http://www.alizila.com/alibabas-big-data-means-counterfeiters-can-run-cant-hide-ipr-enforcement/.

165 Graeme Dinwoodie (n 160).

166 Chen (n 61).

167 Monahan (n 60).

168 Mostert (n 6).

169 Ibid.

remedy where a balancing of interests needs to take place[170], the following is submitted. The allocation of who should do what should be governed first by who has the competence and ability, and then by cost and efficiency in the context of the specific case[171]. This is because the technology in the cyber world develops at lightning speed (in view of Moore's law)[172] and this necessitates a constant and frequent review on a case by case basis of the cost and other factors which will inevitably vary in proportion and composition[173].

V. JURISDICTION AND ENFORCEMENT OF JUDGMENTS

91. Any effective cross-border online enforcement measures, per definition, will require an international approach to jurisdiction. The internet is a global system of interconnected computers[174]. It provides a global window for both brand owners and counterfeiters alike. As Justice Abella of the Canadian Supreme Court so eloquently puts it: "The internet has no borders; its natural habitat is global. The only way to ensure the interlocutory injunction [order] attained its objective was to have it apply where Google operates – globally."

92. An important recent development that underscores the importance of global enforcement of judgments is the Canadian Supreme Court's decision in *Google Inc v Equustek Solutions Inc.*[175]. The Supreme Court upheld an injunction prohibiting Google from delivering search results pointing to the defendants' websites selling counterfeit goods across all of Google's websites globally. Central to the judgment was the notion that the global nature of the infringement medium, the internet, required a remedy that was not territorial but had a cross-border, international application. Delivering the majority judgment, Justice Abella rejected Google's argument that it was improper for the injunction to have extraterritorial effect, noting: "The interlocutory injunction in this case is necessary to prevent the irreparable harm that flows from Datalink carrying on business on the internet, a business which would be commercially impossible without Google's facilitation. The order targets Datalink's websites – the list of which has been updated as Datalink has sought to thwart the injunction – and prevents them from being displayed where they do the most harm: on Google's global search results"[176]. In the United Kingdom, a similar principle of law has been recognized outside the IP context in *Re J*[177]. Sir James Munby held that "there is, in principle, no objection to the English court in an appropriate case granting a *contra mundum* injunction against the world at large, including against foreign-based internet website providers". Both these decisions suggest a growing international recognition of the importance for the cross-border enforcement of injunctions in relation to the internet.

93. Below is an outline of the current framework for cross-border judicial co-operation in the enforcement of IP judgments, and options for reform[178].

---

170 *eBay Inc. v. MercExchange, L.L.C*. 547 U.S. 388 (2006).

171 Anne Gundelfinger, Vice President, Global Intellectual Property, Swarovski, Past President International Trademark Association, (personal communication, July 28, 2017).

172 Gordon E Moore, 'Cramming More Components onto Integrated Circuits' (1998) 86 *Proceedings of the IEEE* 82.

173 Anne Gundelfinger (n 171).

174 <https://www.igi-global.com/dictionary/internet/15369> accessed 1 August 2017.

175 *Google Inc. v Equustek Solutions Inc.*, 2017 SCC 34.

176 Ibid [42] (Abella J).

177 [2013] EWHC 2694 (Fam).

178 See also WIPO/ACE/12/7 and WIPO/ACE/12/8; Andrew F. Christie, Private International Law Issues in Online Intellectual Property Infringement Disputes with Cross-Border Elements - An Analysis of National Approaches (WIPO, 2015) http://www.wipo.int/publications/en/details.jsp?id=3975&plang=EN.

94. As Asensio[179] points out, beyond regional organizations, there has been little success in creating international frameworks dealing with the recognition and enforcement of IP disputes. Existing multilateral treaties, such as the TRIPS Agreement, fail to cover cross-border recognition and enforcement of judgments. No harmonized standard currently exists globally. Consequently, rules on recognition and enforcement vary greatly depending on the law of the country where enforcement is sought. For example, there are fundamental differences to the importance of reciprocity in determining whether judgment from a particular country is capable of being recognized[180]. Similarly, there are key differences in whether certain types of judgments, such as non-monetary judgments like inunctions, are capable of being enforced[181]. The lack of clear rules regarding non-monetary judgments is of particular concern given that injunctive remedies are an integral tool to fight counterfeiting in the online environment. Thus, even if a rights holder secures a favorable judgment in one jurisdiction, they may not have an easy way to enforce these rights in a foreign jurisdiction, which will cause delay and costs.

95. The clear importance of developing a common framework for cross-border judicial enforcement of IP disputes has driven proposals for legislative reform. Key proposals include the American Law Institute's "Principles Governing Jurisdiction, Choice of Law, and Judgments in Transnational Disputes", the European Max Planck Group on Conflict of Laws in Intellectual Property's "Principles for Conflict of Laws in Intellectual Property" and the Japanese Transparency Proposal on Jurisdiction, Choice of Law, Recognition and Enforcement of Foreign Judgments in Intellectual Property. As has been highlighted, despite differences in approach, reform proposals share a common core goal: enhancing the recognition and enforcement of judgments. In a nutshell, these proposals seek to adopt an expansive definition of judgment in respect of both enforcement and recognition, encompassing both default judgments as well as non-monetary judgments. Similarly, in the European Union, the European Court of Justice has recently underscored the importance of adopting a broad understanding of the concept of "judgment" to enhance mutual recognition and enforcement[182]. It should be noted that at present, the Hague Conference is working on a Convention which it is hoped will include judgments in IP cases, but the agreed scope may not extend to injunctions[183].

96. Beyond issues of jurisdiction, cost and duration are also factors important to the effectiveness of enforcement proceedings. This is especially true in view of the volume and velocity of counterfeits on the internet. A recent promising initiative has been the launch of an online court in China dedicated to hearing e-commerce and online IP infringement disputes[184]. The online court allows both pre-trial mediation proceedings and litigation to be conducted via

---

179 Pedro A. De Miguel Asensio, "Recognition and Enforcement of Judgments: Recent Developments", *Research Handbook on Cross-border Enforcement of Intellectual Property* (2014). //www.elgaronline.com/9781781955796.00017.xml. See also Pedro A. De Miguel Asensio, "Recognition and Enforcement of Judgments in Intellectual Property Litigation: The CLIP Principles", in Jürgen Basedow, Toshiyki Kono and Axel Metzger (eds), *Intellectual Property in the Global Arena – Jurisdiction, Applicable Law, and the Recognition of Judgments in Europe, Japan and the US*, Mohr Siebeck (2010), pp. 239–292; and Pedro A. De Miguel Asensio, "Part 4: Recognition and Enforcement", *Conflict of Laws in Intellectual Property (The CLIP Principles and Commentary)*, OUP (2013), pp. 388–468.

180 China places great importance on reciprocity, making it an outlier compared to most other nations. Wenliang Zhang, "Recognition and Enforcement of Foreign Judgments in China: A Call for Special Attention to Both the Due Service Requirement and the Principle of Reciprocity" (2013) *Chinese Journal of International Law*, vol. 12, pp. 143–174.

181 Pedro (n 63).

182 C-456/11, *Gothaer*, [2013] 2 W.L.R. 520; [2013] C.E.C. 793; [2013] I.L.Pr. 7.

183 See 'The Work Of The Hague Conference On Private International Law In Relation To The Cross-Border Enforcement Of Intellectual Property Rights' in WIPO/ACE/12/8 (2017).

184 Dani Deahl, 'China launches cyber-court to handle internet-related disputes' (*The Verge*, 18 August 2017) https://www.theverge.com/tech/2017/8/18/16167836/china-cyber-court-hangzhou-internet-disputes accessed 23 Augustl 2017.

livestream, allowing disputes to be resolved more quickly and at lower cost than physical proceedings[185].

97. In sum, with civil remedies against online infringers, two key issues arise that substantially affect enforcement of IP rights online. The first is the issue of jurisdiction. At present it is unclear how strong a connection there must be with a specific jurisdiction in order for a court to accept jurisdiction. Online counterfeit cases will have a varied degree of "connection" with the jurisdiction in which the right holder is trying to enforce its rights (for example, is the presence of the website targeting the consumers in that jurisdiction sufficient?). Second, issues of enforcement of judgments are not regulated in a global way to correspond to the global nature of the infringement medium. Right holders with favorable judgments from one jurisdiction have no easy way to enforce these rights in a foreign jurisdiction and must therefore undergo recognition and enforcement proceedings, which will cause delay and costs.

A. VOLUNTARY ARBITRATION

98. It is of interest to note that the enforcement of foreign arbitration awards in international commercial matters are easily enforced in all jurisdictions – that is to say, in Member States that are signatories to the 1958 New York Convention on Recognition and Enforcement of Foreign Arbitration Awards (the "New York Convention").

99. Few national laws on arbitration or IP explicitly allow for the arbitration of intellectual property disputes[186], but almost no national laws explicitly forbid the arbitration of intellectual property disputes[187]. Key exceptions expressly providing for the arbitrability of IP disputes include the United States[188] and the European Union which recognize that patent disputes can be arbitrated with *inter partes* effect[189], Belgian law which provides for patent arbitration with both *erga omnes* and *inter partes* effect[190], and Swiss law which extends this recognition to all IP rights[191]. Most arbitration and IP legislation does not contain any reference to the arbitration of IP disputes at all. Accordingly, they tend to be treated the same way as other commercial disputes, and an arbitral tribunal's determinations regarding validity of IP rights are generally understood to be effective *inter partes* but not *erga omnes*. In some cases, however, uncertainty about the ability to arbitrate IP cases may be rooted in skepticism as to whether what is essentially a private agreement between parties can result in private, non-governmental actors making decisions on the validity of a state-granted property right. Yet, as the WIPO Arbitration and Mediation Center notes, this is "generally a non-issue in most jurisdictions"[192]. Moreover, disputes regarding online counterfeits primarily center around the infringement of trademark rights, which is distinct from a dispute about the validity of the trademark as a

---

185 While not specific to intellectual property or internet disputes, other promising initiatives in this vein have been the launch of an online court pilot program in the United Kingdom, and an online tribunal for small claims disputes in Canada. See Dan Bindman, 'Plan for 28-month Online Court pilot emerges as MR foresees live-streaming Court of Appeal' (*Legalfutures*, 23 June 2017) http://www.legalfutures.co.uk/latest-news/plan-28-month-online-court-pilot-emerges-mr-foresees-live-streaming-court-appeal accessed 23 August 2017.

186 Trevor Cook, 'Alternative Dispute Resolution (ADR) as a Tool for Intellectual Property (IP) Enforcement', WIPO/ACE/9/3 (2014).

187 A rare exception is South Africa. Article 18(1) of the Patents Act 1978 states: "Save as is otherwise provided in this Act, no tribunal other than the commissioner shall have jurisdiction in the first instance to hear and decide any proceedings, other than criminal proceedings, relating to any matter under this Act."

188 35 U.S.C. 294 (Voluntary arbitration).

189 Article 35 of the Agreement on the Unified Patent Court of 19 February 2013, OJEU C175 20.6.2013.

190 Article 51(1) Belgian Patents Act.

191 Decision of the Swiss Federal Office of Intellectual Property dated 15 December 1975.

192 WIPO Arbitration and Mediation Center – *Update on the WIPO Arbitration and Mediation Center's Experience in the Resolution of Intellectual Property Disputes* (LES Nouvelles 2009, pages 49–54). There is, however, a certain amount of uncertainty as to the arbitrability of the validity of registered IP rights in Indian law.

registered right, sidestepping concerns about whether an arbitration award in this context would have an *erga omnes* effect.

100. The key benefit arbitration offers to address the challenge of online counterfeiting is that it provides an efficient mechanism to resolve multi-jurisdictional disputes. As noted earlier, given the global nature of the infringement medium of the internet, disputes surrounding counterfeit goods can encompass the intellectual property rights of several different countries. This eliminates the need for right holders to pursue multiple parallel proceedings, reducing costs and the time required to resolve disputes.

VI. CRIMINAL MEASURES

101. As Anne Gundelfinger astutely notes, counterfeiting is fundamentally different from typical IP disputes[193]. Unlike routine forms of IP infringement, counterfeiting rarely raises a question as to the validity and scope of the IP rights. From this perspective, counterfeiting is not conceived primarily as a problem of property stolen or infringed, but of fraud and breach of public interests in which consumers and ultimately economies are massively harmed, in addition to the right holder. Moreover, as a form of fraud, counterfeiting raises no tenable fair use or free speech issues[194]. Thus, stepping outside a civil intellectual property framework and relying on criminal law may be key to identifying uniform and efficient transnational solutions.

102. In line with this view, right holders have attempted to combat counterfeiting with the help of criminal law. Especially when counterfeiting sales reach a certain threshold, law-enforcement agencies will assist with prosecution of the counterfeiter and stop these illegal operations. In some jurisdictions law-enforcement agencies have specialized units that deal with counterfeit goods, particularly on a significant commercial scale.

103. In the UK, law-enforcement agencies are guided by the IP Enforcement 2020 policy document which lays out key strategic thrusts to tackling counterfeiting[195]. Counterfeit sales are investigated by the Police Intellectual Property Crime Unit (PIPCU) at City of London Police[196]. Criminals are using the internet as a sales tool, with professionally designed, realistic looking websites whose sole purpose is to fool victims into believing they are purchasing legitimate goods. To combat this emerging threat the PIPCU created Operation Ashiko. This operation specifically targets the sale and distribution of counterfeit websites with a focus on the .uk ccTLD. Core to the operation is a collaboration with Nominet, the body responsible for the registration of ".uk" domains. PIPCU provides Nominet with a monthly list of vetted domains verified by industry as being involved in the sale of counterfeit goods to suspend and lock domain names connected to the sale and distribution of counterfeit products online.

104. To ensure the swift removal of illicit websites, the City of London Police in conjunction with Nominet have agreements in place to suspend illicit websites within the .uk parameters without the need of a court order. This agreement is on the mutual understanding that PIPCU will carry out strict due diligence assessing counterfeit websites on the internet, which have been linked to fraud and IP offences.

---

193 Anne Gundelfinger (n 171).

194 See para [44] – [45] above.

195 United Kingdom Intellectual Property Office, 'Protecting Creativity, Supporting Innovation: IP Enforcement 2020https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/571604/IP_Enforcement_Strategy.pdf accessed 19 July 2017. See also WIPO, Advisory Committee on Enforcement: E Jones, 'UK Experience on Tackling Online IP Infringement' (9 January 2014) WIPO/ACE/9/22, [3].

196 City of London Police, 'Counterfeit Goods' (20 February 2017) https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/Pages/counterfeit-goods.aspx accessed 17 July 2017.

105. Yet, a continuing challenge facing law enforcement in tackling online counterfeiting is the ease with which counterfeiters can register new website domains to sell fake goods. Counterfeiters often rely on false WHOIS data (information on registered users of domain names) or fraudulent identities harvested from unsuspecting consumers. Existing preliminary checks required by domain name registrars often fail to screen such false data out. To address this challenge, considerations are being given to exploring the potential of using global money laundering legislation as a complementary tool to tackle online counterfeiting.

106. Due to global money laundering legislation, major global merchants and payment facilitators require businesses to carry out thorough due diligence checks called "Know Your Customer" (KYC's)[197]. This requires firms to take steps to demonstrate that any funds they receive do not originate from criminal activity and do not facilitate money laundering. This legislation could equally apply in the context of global domain-name registrars that counterfeiters use to register websites selling fake goods. Currently, upon receiving notice that a website is registered by a counterfeiter, domain-name registrars must remove the counterfeit website to enjoy protection under safe-harbor rules. However, if domain-name registrars continue to knowingly permit the same organized crime groups to register websites selling counterfeit goods despite having specific notice of infringement, they may no longer enjoy immunity under safe-harbor. Therefore, any such funds received may in principle be subject to money-laundering legislation, and uncooperative registrars could face additional scrutiny regarding the adequacy of the due diligence procedures they have adopted.

107. In this regard, "whitelists" could be explored as a tool to help global domain-name registrars tackle fraudulent registrations and comply with the due diligence requirements imposed by money-laundering legislation.

108. However, it is important that implementing enhanced "Know Your Customer" requirements be balanced against countervailing free-speech interests. Unlike with criminal counterfeiting, there are important situations where the anonymity of lawful speech must be protected, especially in the context of expressive, non-commercial speech. As Terri Chen points out, in the United States courts have held that registering domain names as brands for the purpose of criticizing or commenting on those brands is not a violation of trademark law, and that the registrants of those domain names may properly remain anonymous under some circumstances[198]. However, the putative free-speech interest must be genuine, and not a mere pretext for commercial advantage[199].

109. In the context of the proliferation of online counterfeits worldwide, it should also be noted that in corporate governance and international industry circles ICANN's important role is being considered. The support which ICANN and domain name registrars may be able to offer should be looked at in view of their global remit and responsibility to the international internet community. This is particularly so as the current dilemma of online counterfeits are often enabled by false domain name registrant information. The problem is one of commercial fraud, which in accordance with traditional legal principles should require a higher level of due diligence and registrant disclosure.

---

197 In the United Kingdom, Money Laundering Regulations 2007. See generally USA Patriot Act 2001; The Anti-Money Laundering and Counter-Terrorism Financing Act 2006; Namibian Financial Intelligence Act 2012; South African Financial Intelligence Centre Act 38 of 2001.

198 *Sermo, Inc. v. CatalystMD, LLC Case No. D20080647.*

199 *Walmart Stores, Inc. v. Walsucks and Walmarket Puerto Rico*, Case No. D20000477. See generally, "WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Second Edition" http://www.wipo.int/amc/en/domains/search/overview2.0/#24 accessed 3 August 2017.

110. In China, co-operation with law-enforcement authorities is possible, but it is more likely to yield results when the IP owner co-operates in the investigation by providing information and showing interest in the progress of the investigation[200]. Attempts to assist with the efficiency of criminal enforcement measures continue to develop, as demonstrated by the 2014 Judicial Interpretation on Criminal Procedural Rules for Internet Crimes, issued by the Supreme People's Procuratorate and the Ministry of Public Security[201]. In the Republic of Korea, the Korean Intellectual Property Office created the Special Investigative Police for Trademark to enhance law enforcement on counterfeits[202].

111. Concerns of illicit trade are particularly sensitive in areas such as pharmaceuticals, where human life is at risk[203]. On global and transnational levels, agencies like INTERPOL and EUROPOL[204] are taking specific initiatives and organize task forces, to combat trafficking in illicit goods.

VII. ADMINISTRATIVE AND CUSTOMS PROCEEDINGS

112. Complementing regimes of civil and criminal enforcement, many jurisdictions grant administrative and customs remedies available to rights holders to stop infringement of their IP rights.

113. In China, administrative departments for industry and commerce are responsible for the supervision and administration of online commodity trading[205]. Third-party trading online platforms have the duty not only to monitor their websites for IP infringement[206], but also to report[207] potential infringements to authorities and assist these authorities in "investigating and punishing illegal online business operations" by providing registration information, or any other information on the infringer[208]. If a violation of this obligation is found, administrative authorities have the power not only to inquire and investigate, but also to seize counterfeit goods and business assets; close the business premises; or request the shutdown of the website selling fakes[209].

---

200 http://www.worldtrademarkreview.com/Intelligence/Anti-counterfeiting/2016/Country-chapters/China.

201 Ibid.

202 See "Institutional Arrangements Put in Place in the Republic of Korea to Address the Proliferation of Counterfeit Goods Online" in WIPO/ACE/12/10.

203 Counterfeits of pharmaceuticals attracted concerted efforts of INTERPOL and 115 countries worldwide – Operation Pangea VIII (Report 18 June 2015). Described as a "major threat to public health" – INTERPOL, https://www.interpol.int/Crime-areas/Pharmaceutical-crime/Pharmaceutical-crime.

204 See "Institutional Arrangements to Address Online Intellectual Property Infringements – Europol's Experience" in WIPO/ACE/12/10.

205 Art. 39 Administrative Measures for Online Trading (State Administration for Industry and Commerce, 2014). Discussed also in Ferrante, 260.

206 If there is a notice of infringement by the IP holder, the intermediary has to take all necessary measures under the Tort Law to stop such infringement – Art. 27 Administrative Measures for Online Trading (State Administration for Industry and Commerce, 2014).

207 Art. 26 Administrative Measures for Online Trading (State Administration for Industry and Commerce, 2014) – any violations should be reported to local administrative authorities.

208 Art. 34 of Administrative Measures for Online Trading (State Administration for Industry and Commerce, 2014); if obligation is not met, a financial fine can be imposed (Article 50).

209 Arts 43 and 46 (request to be made to communications administrative department licensing or filing the operation of a website) Administrative Measures for Online Trading (State Administration for Industry and Commerce, 2014).

114. Another remedy, which is regularly used by some right holders[210], is the domain-name seizure procedure (specifically available in the EU and the US)[211]. Once seized, the domain names are regularly used to educate and raise awareness of the consumers about intellectual property crime. When available, this remedy is particularly useful in cases where infringed trademarks are copied in the domain name itself. If trademarks do appear in the domain name itself, the easier way to enforce trademark rights is the dispute resolution procedure as available under the Uniform Domain Name Dispute Resolution Policy (UDRP)[212].

115. Finally, trademark owners will also co-operate with customs authorities to stop counterfeit trading. In the EU, a right owner can stop counterfeit sales even when a consumer bought a counterfeit product through an online platform based outside the EU[213]. In addition, the EU Enforcement Database (EDB) has been established to assist customs officials and law enforcement in stopping counterfeit trading. The EDB contains information on products that have been granted an IP right, like a registered trademark. This information can then be accessed by law-enforcement and customs officials throughout the European Union, making it easier to identify counterfeits and take action. Moreover, for right holders, it functions as prima facie evidence of ownership of rights relating to their products, which helps right holders more easily submit take-down notices on counterfeit listings online.

VIII. IMPORTANCE OF BLACKLISTING, DELISTING AND WHITELISTING[214]

116. As part of` an overall solution, the importance of blacklisting or delisting and whitelisting should be considered[215]. Blacklists refer to lists of repeat offenders that government authorities, law enforcement authorities, right holders, platforms, domain name registrars, and trade mark registries share to pinpoint and pull together the jigsaw puzzle of local or international counterfeit crime networks. For example, the New York Police Department led by New York Police Commissioner Kelly demonstrated how successful blacklisting works in practice when sharing information on counterfeit sources which lead to counterfeit crime groups[216]. Trademark law already contains the prohibition of trademark registration in bad faith – and this principle

---

210 Presented in WIPO, Advisory Committee on Enforcement: C. Aubert, "The Activities of the Federation of the Swiss Watch Industry in the Area of Preventative Actions to Address Online Counterfeiting" (31 July 2015). WIPO/ACE/10/22, [13] (recovered domains are then used to increase consumer awareness).

211 In the US conducted by Immigration and Customs Enforcement Agency (ICE), and in the EU by Europol. See "The Role of the National Intellectual Property Rights Coordination Center in Enforcing Intellectual Property in the United States of America" in WIPO/ACE/11/8 and Europol's Experience in WIPO/ACE/12/10. See also the mention of the seizure of several hundred domain names by the Public Prosecutor in Denmark in Knud Wallberg, "Recent Developments in Domain Name Law and Practice under the .dk Top Level Domain", NIR 1/2017, p. 39 f.

212 http://www.wipo.int/amc/en/domains/gtld/ accessed 1 August 2017.

213 *Blomqvist v Rolex SA and another*, Case C-98/13, ECLI:EU:C:2014:55.

214 See also Mostert and Asokan (n 9).

215 The process of creating whitelists and blacklists of safe and unsafe internet addresses is widely used by ISPs and many agencies which work in enforcement. Domain names are the internet's signposts, which consumers trust to lead them to authentic content, naturally expecting that the owner of "BrandX.com" is the owner of the trademark "BrandX". Most domain names connected to the internet have a Whois record, which often features the registrant name, an administrative, billing and technical contact plus the servers on which the domain is hosted as well as the registrar which provisioned the domain. Although it is possible to mask the registrant's details behind a privacy curtain or to fabricate all contact details, the registrar that provisioned the domain will have the credit card details of the registrant. A small number of agencies have developed technologies and processes to validate domain applicants, making sure that "the right name gets to the right person" during registry launch processes such as .Wales and to verify whois records post-registration to ensure on-going conformity to registry formalities such as nexus requirement within the European Union in the case of .EU or continuing professional certification in the case of .Law or .Abogado. There is substantial best practice that can be built upon. Provided validation is carried out on a regular basis, whitelists of authentic addresses are effective whilst blacklists, provided there is a clear mechanism to be removed from a Black list after a verification check, can significantly reduce on-line abuse.

216 New York Police Department Criminal Enterprise Division.

could be explored further in the context of online counterfeit sales[217]. Blacklists could serve as a very useful tool for intermediaries and authorities that have to confront repeat offenders on a daily basis.

117. One possibility would be to render blacklisting consistent with existing legislation[218]. For instance, in China, businesses that have had their trademarks successfully opposed or revoked more than a certain number of times in a certain number of years are potential candidates for blacklisting[219]. The significance of being placed on a blacklist could vary. Possible suggested effects might include: (1) additional scrutiny to be placed on blacklisted entities' attempts to list goods for sale; (2) additional penalties to be imposed if a blacklisted entity has its trademark revoked or opposed for bad-faith registration.

118. In the context of voluntary measures, the online platform Alibaba, for example, has recently introduced blacklisting to help tackle infringement. Alibaba's rules strictly ban the practice of merchants opening multiple, dummy storefronts using borrowed, purchased or fake identity cards. First implemented on Taobao, these rules were later extended to all Alibaba platforms in November 2016. After these rules went into effect, big-data technology was employed to scan all new and existing Taobao accounts. New accounts identified as creating fake storefronts to sell suspicious goods were banned from Alibaba's platforms, whereas existing account owners identified as IP infringers were subject to harsher penalties, the severity of which was determined by the gravity of the offence.

119. The inverse, i.e. the use of whitelisting, is of equal importance to combat counterfeits in the online world. An online "opt out" database[220] for the registration of domain names could be established where members of the public would be able to register their authentic details. Upon an application for a domain name, registrars would screen the registrant's details against the database to confirm if they are authentic and if the individual has opted out of domain name registrations. If an individual has opted out, the registration would fail, protecting members of the public from identify fraud and restricting the ability of counterfeiters to register websites selling counterfeit goods. This approach is aligned with existing initiatives in the electoral and banking context which require stringent due diligence checks to protect consumers from fraud[221].

120. It should be noted that any "whitelists" introduced must clearly be limited to serving solely as a reference point and checklist of authentic versus counterfeit for platforms, domain name registrars, law enforcement and administrative authorities to use as a source and provenance reference. Whitelists should not be used to control distribution or interfere with the sale of genuine goods.

---

217 Blacklisting proposed more generally as part of remedying bad-faith trademark registrations in China – F. Mostert and G. Wu, "The Importance of the Element of Bad Faith in International Trade Mark Law and its Relevance Under the New Chinese Trade Mark Law Provisions" (2017) *JIPLP* 1.

218 Ibid., 9.

219 H.D. Wan, "SAIC to Blacklist Businesses for Serious Trade Mark and Unfair Competition Law Violations", http://www.lexology.com/library/detail.aspx?g=369960af-6fb4-47b7-96e0-8375dc43aba1 accessed 2 March 2017.

220 See (n 215).

221 UK Government, 'The electoral register and the 'open register' (2017) https://www.gov.uk/electoral-register/opt-out-of-the-open-register accessed 1 August 2017. See also CIFAS, 'Protective Registration' (2017) https://www.cifas.org.uk/services/identity-protection/protective-registration accessed 1 August 2017.

IX. CONCLUSION

121. The proper protection and enforcement of trademark rights online still lacks effective, joined-up enforcement measures. In a number of jurisdictions right holders can avail themselves of civil, administrative and criminal remedies, but their efficiency in the future depends on a voluntary, collaborative approach. Online trademark counterfeits are international by nature. Consequently, the existing international cooperation mechanisms, such as cooperation through mutual legal assistance agreements or international arrest or evidence warrants, are lengthy processes and inadequate to respond to large volume, high speed and anonymous online counterfeit activities.

122. As it stands now, the better options are the further development of common approaches on voluntary measures, criminal measures, jurisdiction, arbitration and the appropriate standards and responsibilities for intermediaries in accordance with the international “ratio” principles. In fact, it is important to note that de facto guidelines have already developed around the world where right holders, intermediaries and government law enforcement authorities have voluntarily cooperated with each other and across borders to effectively combat online counterfeits. These measures are in need of further evolution and guidance because the internet is by its nature global. Effective measures are dependent on voluntary, collaborative technical and legal standards.

[End of document]