E

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

WIPO/ACE/14/7
ORIGINAL: ENGLISH
DATE: JULY 23, 2019

Advisory Committee on Enforcement

Fourteenth Session
Geneva, September 2 to 4, 2019

STUDY ON IP ENFORCEMENT MEASURES, ESPECIALLY ANTI-PIRACY MEASURES IN THE DIGITAL ENVIRONMENT[*]

Document prepared by Dr. Frederick Mostert, Professor of Practice at the Dickson Poon School of Law, King's College, London, Research Fellow at the Oxford Intellectual Property Research Centre, and Ms. Jane Lambert, Barrister, Gray's Inn, London[**]

ABSTRACT

This study provides an overview of current approaches to online copyright infringements, focusing specifically on the responses to piracy in the digital sphere across the world. The study explores the global problem of online piracy, the different types of digital tools and administrative measures used by rights holders, online platforms, governments and the judiciary. These digital tools and measures include blocking, notice and takedown, notice and staydown, filtering and monitoring, Bad Actor[1] listings, "follow-the-money" principle, public awareness initiatives, codes of conduct and voluntary guidelines, and digital authentication tools such as Blockchain. The study incorporates a discussion on the issues concerning anonymity and the "whack-a-mole" problem and notes the challenge of balancing fundamental rights such as freedom of expression and data privacy rights and the protection of copyright. The study highlights the gaps within the legal measures used at present and current discussions around a possible uniform approach in the form of global guidelines in response to the present dilemma.

[*] This study was undertaken with the aid of funds provided by the Ministry of Culture, Sports and Tourism of the Republic of Korea. Apologies for any shortcomings which may remain - the responsibility for which are the authors' alone. Our gratitude to Marija Nonkovic, LLB, King's College London, for her tremendously helpful research and contribution to this study. The authors are also indebted to the most insightful inputs from Maria Fredenslund, Mr. Justice Arnold, Anne Gundlefinger, Matthew Bassiur, Nick Wood, Cedric Manara, Weizmann Jacobs, Ik Hyun Seo, Alex Urbelis, Tim Trainer and Marty Schwimmer.

[**] The views expressed in this document are those of the authors and not necessarily those of the Secretariat or of the Member States of WIPO.

[1] "Bad Actor" is a term commonly used in the online world for actors involved with illicit activities.

I. INTRODUCTION

1. Digital technology is arguably humankind's greatest achievement since the printing press. Thanks to Big Tech and the advent of platforms such as Google, Alibaba, Amazon, Facebook, and Twitter, the way we live, search for things, shop and communicate have all changed fundamentally[2].

2. Digital technology has freed up our time from manual tasks; it enables us to keep in touch globally and to be informed on a scale never experienced in history. But as we open our houses to ever more interconnected technology, as governments ponder the idea of "smart cities", and as the hunger for convenience and speed push caution to one side and increase our attack surface, the same technology we are embracing carries risks for us in multiple ways. A case in point is the efficient way in which Bad Actors use technology to flood the platforms and online markets with pirated content.

3. This report seeks to present the ways in which enforcement measures have been adapted to meet the challenge of online copyright infringement.

II. THE CHALLENGES OF THE DIGITAL ENVIRONMENT

4. The volume and frequency of online activities are unprecedented. The law has traditionally lagged behind commercial and technological development. Courts and legislatures around the world have had difficulty in dealing with the actions of Bad Actors online.

5. Existing solutions in the digital environment often subject to intractable challenges. First, the identity of the pirate is often unknown to the content owner. Second, the anonymity problem exacerbates the "whack-a-mole" phenomenon – where a webpage is taken down and another online listing pops up under a different URL almost instantly. Third, the sheer volume and velocity of online counterfeit sales make online listings very time sensitive – they are typically posted for a few hours or days only, making timely online tracking and tracing of pirate listings extremely difficult. Fourth, pirates typically use more than one website in different countries. This raises questions of international jurisdiction and the enforcement of foreign judgments. And fifth, there is no uniform, international mechanism for sharing information by law enforcement on online pirate identities.

6. The procedures and remedies that Part III of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) requires were appropriate for tracing and intercepting CDs, cassettes and other physical objects. The digital age has changed the nature of the threat of piracy. Issues specific to online piracy include that infringing content can be accessed at the click of a button. Unlike the sale of counterfeit goods online, a customer does not need to wait for the products to be delivered but can download or stream illegal content instantly. Once accessed, the copyright protected material can be processed, stored and disseminated globally. They cannot be impounded at borders or recovered upon the execution of a search order. The intangible nature of the material coupled with an Internet without boundaries between countries has resulted in the volume and velocity of copying. It makes no sense for a content owner to run to court – at great expense – to stop the single sale of a pirated content on a digital platform because the actual listing typically appears online for only a few hours. Moreover, such action does nothing to address the multitude of other illegal listings posted by other Bad Actors.

---

[2] https://www.wipo.int/wipo_magazine/en/2018/si/article_0005.html.

7. One of the root causes of the difficulty in dealing with nefarious activity on the Internet is anonymity. The cloak of anonymity allows Bad Actors to evade detection. Only if the wrongdoing is systematically tracked and traced to the source of the problem – from the digital world to a physical location – can traditional means of enforcement make any substantive headway.

8. Many agencies are part of an intricate structure to combat piracy at both a local and an international level. Accordingly, this study suggests there is a need for a more coordinated international effort to drive a balanced and effective approach to enforcement.

III. DEVELOPING JUDICIAL RESPONSES TO ONLINE INFRINGEMENT

9. This section discusses some of the forensic remedies that have been adapted by the courts to the online environment, particularly in relation to intermediaries that are referred to in paragraph 7.

A. ORDERING DISCLOSURE OF DOCUMENTS AND INFORMATION

10. The problem of identifying wrongdoers mentioned above can sometimes be solved by an order for the disclosure of documents or information. Article 43.1 of the TRIPS Agreement requires WTO members to authorize judges to order parties possessing specific evidence relevant to the substantiation of the claims made in the action to produce such evidence to the claimant. Article 47 of this Agreement provides that parties may empower the courts to order the infringer to inform the right holder of the identity of third persons involved in the production and distribution of infringing goods or services and of their channels of distribution.

11. In countries of the common law tradition, the courts have power under general principles to order persons who are caught up innocently in wrongdoing to disclose documents or give information identifying wrongdoers or revealing the precise nature and full extent of the wrongdoing. Not every country of the civil law tradition has such a procedure. However, the EU Enforcement Directive, recognizing the particular requirements of litigation in IP cases, provides in Article 8 for a right of discovery against infringers as to the sources and channels of distribution of infringing goods[3]. In France, for example, the saisie-contrefaçon is a procedure under which the court may order the examination of premises and documents by a bailiff[4].

12. The jurisdiction in the United States to make orders for discovery was noted by Lord Denning in Norwich Pharmacal Co. and Others v Customs and Excise Commissioners[5], which was the first case in the Commonwealth to consider the issue in modern times. In that case, a patentee sought an order to compel the customs authorities to disclose the names of importers of a substance that was believed to infringe its patent. Speaking in favor of the patentee, Lord Reid said:

> "If through no fault of his own a person gets mixed up in the tortious acts of others so as to facilitate their wrongdoing he may incur no personal liability but he comes under a duty to assist the person who has been wronged by giving him full information and disclosing the identity of the wrongdoers".

---

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

[4] See paragraph 16, below.

[5] [1974] AC 133, [1974] RPC 101, [1973] FSR 365, [1973] 2 All ER 943, [1973] UKHL 6, [1973] 3 WLR 164 (https://www.bailii.org/uk/cases/UKHL/1973/6.html).

13. In England and Wales, orders of this kind have been made against internet chat rooms[6], a social media platform[7] and an online payments processor[8]. In such applications, the party seeking the order usually has to pay the costs[9] of the respondent as well as its own.

14. In Australia, Mr. Justice Perram of the Australian Federal Court ordered several Australian Internet service providers (ISPs) to disclose the names of subscribers who had used the ISPs' facilities to download unlicensed copies of the claimant's film in *Dallas Buyers Club LLC v iiNet Limited* (No 3)[10]. In a similar case in Canada, the applications judge ordered an ISP to disclose the contact details of a subscriber who was believed to have infringed copyright in a film through file sharing. The order for disclosure (which was actually referred to in the report as a "Norwich order") was not challenged, but the question as to who should pay the ISP's costs of complying with the order was referred to the Canadian Supreme Court[11].

B. RECOVERING AND PRESERVING EVIDENCE

15. Article 50.1(b) of the TRIPS Agreement requires WTO members to authorize the judicial authorities to order prompt and effective provisional measures to preserve relevant evidence in regard to an alleged infringement. There is a similar obligation upon EU member states under Article 7 of the Enforcement Directive[12].

16. Article 50.1(b) of TRIPS and Article 7 of the Enforcement Directive are transposed into French law by Article 615(5) of the Intellectual Property Code. That provision enables the president of the superior court of first instance to authorize an officer known as a *huissier* or bailiff to enter, inspect and if necessary seize documents and other evidence relevant to the case. That procedure is known as a *saisie-contrefaçon* in France. In Belgium a similar procedure is known as a *saisie-description*[13].

17. This obligation is discharged in England and Wales by authorizing the courts to grant search orders or, as they are called in other countries of the common law tradition, *Anton Piller* orders. A search order is an injunction[14] requiring the person in charge of business or residential premises or other private space such as an aircraft, ship or vehicle to admit a party of lawyers and experts to such space and allow them to search for, and record or take copies or samples of, any evidence that may be relevant to proceedings that have been or are about to be launched.

18. Whereas under the *saisie contrefaçon* the search is supervised by a court bailiff, in England the search is led by a lawyer from a neutral law firm known as "the supervising solicitor". Other members of the party are likely to be solicitors from the claimant's firm. If computers or other electronic devices are likely to be inspected, the team may include one or more experts in computer forensics. A search order is a draconian order made at the very limits of the court's jurisdiction.

---

6 *Totalise Plc v Motley Fool Ltd and another* [2002] Masons CLR 3, [2002] EMLR 20, [2002] WLR 1233, [2001] EWCA Civ 1897, [2003] 2 All ER 872, [2002] CP Rep 22, [2002] FSR 50, [2002] 1 WLR 1233.

7 *Applause Store Productions Ltd. and another v Raphael* [2008] Info TLR 318, [2008] EWHC 1781 (QB).

8 *Twentieth Century Fox Film Corporation and others v Harris and others* [2014] EWHC 1568.

9 In England and Wales these will usually include solicitors' costs and disbursements as well as counsel's' fees (see *Totalise*, footnote 6 above).

10 [2015] FCA 422 (6 May 2015) (https://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/FCA/2015/422.html).

11 See: *Rogers Communications Inc. v. Voltage Pictures, LLC* [2018] 2 SCR 643.

12 Directive 2004/48/EC, footnote 3 above.

13 See: Article 1369*bis*, Judicial Code (Belgium).

14 Order of the court requiring the person to whom it is addressed to do or refrain from doing something on pain of fine, imprisonment or other punishment for disobedience.

19. The application for an *Anton Piller* or search order is made in the absence of the party whose premises are to be searched. Such orders are made only if the court can be persuaded that the respondent would frustrate the intended proceedings by not disclosing or even hiding, destroying or otherwise putting relevant evidence beyond the reach of the court. The application must be supported by affidavits[15] or affirmations[16] showing not only a strong claim against the respondent for the infringement of an IP right or other wrongdoing but also that the respondent might hide or destroy evidence. Usually that means proving that the respondent has withheld evidence or otherwise acted dishonestly or improperly in the past, or that he or she has a strong incentive to do so in the circumstances. The applicant has a duty to make full and frank disclosure of all relevant facts and matters, whether favorable to its case or not, including any submissions that could have been made by the respondent had he or she been represented before the court.

20. The supervising solicitor serves the order, application, supporting evidence and court transcript on the person or persons in charge of the premises and explains its effect in everyday language. The respondent is allowed a reasonable opportunity to seek legal advice provided that he or she does not frustrate or delay the search unduly. Once they are admitted to the premises, the applicant's solicitors and experts conduct their search. The supervising solicitor makes sure that they act strictly in accordance with the order and with due regard to the rights of the respondent. At the end of the search, the supervising solicitor reports in writing to the court. The court considers the report at a hearing that takes place a few days after the search. Under the *saisie contrefaçon*, the bailiff similarly makes a report to the court as to the results of the search.

21. Search orders were sought frequently when infringing copies of films, games or sound recordings were recorded on discs or tapes that could be intercepted in storage or transit. There has been less scope for such orders now that piracy takes place online. Nevertheless, there are still circumstances when searches can be useful. Search orders are expensive to obtain and execute and applicants risk being ordered to compensate the respondent in damages if the court decides that the order should never have been sought. For all that, they remain a useful remedy. A successful search can have a devastating psychological effect on the willingness of an infringer to resist a claim or persist in wrongdoing. Search or *Anton Piller* orders have been granted in Australia[17], Canada[18], Hong Kong[19], India[20], Ireland[21], New Zealand[22] and Nigeria[23]. In the USA §503(a) of the Copyright Act[24] implements Article 50.1(b) of the TRIPS Agreement, providing for a power in the court to order the impounding of infringing copies, plates and other practices and records documenting the manufacture, sale, or receipt of things involved in the alleged infringement.

---

15 Statements sworn before a solicitor or other commissioner of oaths.

16 Statements affirmed before a solicitor or other commissioner of oaths.

17 *Re Television Broadcasts Limited and others v Thi Phuong Nguyen and others* [1988] FCA 456 (http://www8.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/FCA/1988/456.html?stem=0&synonyms=0&query=Television%20Broadcasts%20Limited%20and%20Nguyen).

18 *Celanese Canada Inc. v. Murray Demolition Corp*., [2006] 2 SCR 189, 2006 SCC 36 (CanLII) (https://www.canlii.org/en/ca/scc/doc/2006/2006scc36/2006scc36.html).

19 Abbott GmbH & Co KG v Pharmareg Consulting Co Ltd [2009] HKCU 549.

20 *Bucyrus Europe Limited and another v Vulcan Industries Engineering* 14 Oct 2004 Kolkatta High Court (https://www.casemine.com/judgement/in/56096030e4b01497112cc1c1).

21 *Microsoft v. Brightpoint* [2000] IEHC 194; [2001] 1 ILRM 540 (July 12th, 2000) (https://www.bailii.org/ie/cases/IEHC/2000/194.html).

22 *Busby v Thorn EMI Video Programmes Ltd* [1984] 1 NZLR 461.

23 *Ferodo Ltd. v Unibros Stores* [1980] FSR 489.

24 17 USC, § 503(a).

C. DAMAGES

22. Article 45.1 of the TRIPS Agreement requires WTO members to authorize their judicial authorities to order an infringer to pay the right holder damages adequate to compensate for the injury the right holder has suffered because of an infringement of that person's IP right by an infringer who knowingly, or with reasonable grounds to know, engaged in infringing activity.

23. This obligation is implemented in the EU by Article 13 of the Enforcement Directive, which requires member states to "ensure that the competent judicial authorities, on application of the injured party, order the infringer who knowingly, or with reasonable grounds to know, engaged in an infringing activity, to pay the right holder damages appropriate to the actual prejudice suffered by him/her as a result of the infringement." That provision is supplemented as follows:

> "When the judicial authorities set the damages:
>
> (a) they shall take into account all appropriate aspects, such as the negative economic consequences, including lost profits, which the injured party has suffered, any unfair profits made by the infringer and, in appropriate cases, elements other than economic factors, such as the moral prejudice caused to the right holder by the infringement; or
>
> (b) as an alternative to (a), they may, in appropriate cases, set the damages as a lump sum on the basis of elements such as at least the amount of royalties or fees which would have been due if the infringer had requested authorisation to use the intellectual property right in question*".*

24. In the case of infringers who did not know, or had no reasonable grounds to know, that they were engaging in infringing activity, Article 13(2) of the Enforcement Directive permits member states to lay down that judicial authorities may order the recovery of profits or the payment of damages, which may be pre-established.

25. In the USA a successful claimant may be awarded "actual damages" for the loss he or she has incurred and, in some cases, the difference between the claimant's loss and any profits that the defendant may have gained. Alternatively, the claimant can recover statutory damages that can be anywhere from $200 for innocent infringements to $150,000 for willful piracy in respect of each copyright that has been infringed[25]. In the UK and several Commonwealth countries, the courts have power to award such "additional damages" as the justice of the case may require having regard to the flagrancy of the infringement and any benefit accruing to the defendant by reason of the infringement[26].

26. Although the substantive law has not changed, the nature of infringement on the internet has required courts to apply that law in evolving circumstances and often on the basis of incomplete information. For example, in *BI and Another v Aktiebolaget Svensk Filmindustri* (Case B 1540-18) the Swedish Supreme Court had to consider the reasonable remuneration payable as damages (on the so-called *user-principle*) for the making available of a single film to the public over 13 months by streaming. The Supreme Court reduced the damages of SEK 4,000,000 awarded by the Court of Appeal, based on a notional license of unlimited scope and duration, to SEK 400,000, based on multiple factors, such as the duration of the infringement, the legal exploitation of the film, the estimated proportion of legal to illegal acts of consumption and the prices paid for licensed consumption. The claimants also recovered SEK 250,000 for damage to the reputation of the work and loss of profits.

---

[25] 17 USC §504.

[26] See, e.g.: *Absolute Lofts South West London Ltd v Artisan Home Improvements Ltd* [2015] EWHC 2608 (IPEC) (14 September 2015) https://www.bailii.org/ew/cases/EWHC/IPEC/2015/2608.html.

D. PREVENTING REMOVAL OR DISSIPATION OF ASSETS

27. Article 9(2) of the Enforcement Directive provides:

> "In the case of an infringement committed on a commercial scale, the Member States shall ensure that, if the injured party demonstrates circumstances likely to endanger the recovery of damages, the judicial authorities may order the precautionary seizure of the movable and immovable property of the alleged infringer, including the blocking of his/her bank accounts and other assets. To that end, the competent authorities may order the communication of bank, financial or commercial documents, or appropriate access to the relevant information".

28. In every country of the EU except Denmark and the UK, that obligation is implemented by Regulation (EU) No 655/2014 of the European Parliament and of the Council of May 15, 2014, establishing a European Account Preservation Order procedure to facilitate cross-border debt recovery in civil and commercial matters[27]. That Regulation permits the courts of the participating member states to make asset preservation orders.

29. In England and Wales Article 9(2) of the Enforcement Directive is implemented by an order is known as a *freezing injunction*. If the court has reason to believe that a respondent would try to defeat a judgment by hiding, dissipating or removing assets against which judgment could be levied, it can restrict the use and movement of any funds or other assets in the respondent's possession or control beyond what is reasonable for everyday business and living expenses or obtaining legal advice.

30. Like search orders, freezing injunctions are at the very limits of the court's jurisdiction. Applications for freezing injunctions are made in the absence of the respondent and usually before proceedings are issued or served. The court has to be persuaded that there is a strong case against the respondent, that he or she has assets and that he or she has hidden such assets or otherwise acted dishonestly or improperly in the past or is likely to do so in the circumstances. As with applications for search orders, written evidence must be sworn or affirmed before a solicitor or commissioner of oaths. Applicants have a duty to disclose to the court all facts and matters upon which a respondent might be expected to rely. Should a freezing injunction be made it may be served not only on the respondent but also on his or her bankers and any other intermediary holding the respondent's assets. A hearing to review the order usually takes place a few days after execution.

31. Freezing injunctions are expensive to obtain and there is always a risk that the applicant may be ordered to compensate the respondent if the court subsequently decides that the order should never have been made. However, the psychological impact of a freezing injunction on a respondent can be as great as that of a search order. In *Twentieth Century Fox Film Corporation and others v Harris and others*[28], which concerned Newzbin2, a web-based service facilitating downloading from newsgroups, Mr. Justice Barling noted at paragraph [23] of his judgment:

> "On 23 November 2012 the Claimants obtained an interim freezing order against Mr. Harris, K, the Foundation and Mr. E. On November 26, 2012, the present proceedings, together with the freezing order, were served on those Defendants. Two days later, on November 28, 2012, the N[ewzbin]2 website ceased operations".

---

27 OJ L 189, 27.6.2014, p. 59–92 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0655).

28 [2014] EWHC 1568 (Ch)

32. It would appear that it was the service of the freezing injunction on the director and shareholder of the company that controlled the Newzbin2 website which closed it down rather than the blocking order that Mr. Justice Arnold made against British Telecommunications over a year earlier[29].

33. Freezing injunctions are available in most Commonwealth common law countries, but not in the USA. In *Grupo Mexicano de Desarrollo, S. A. v. Alliance Bond Fund, Inc.*[30], the US Supreme Court specifically disclaimed jurisdiction to grant asset freezing injunctions.

E. CROSS BORDER INJUNCTIONS

34. A partial solution to the problem of "international jurisdiction and the enforcement of foreign judgments" mentioned in paragraph 5 above is the *kort geding* or trans-border injunction developed by the Dutch courts. In *Lincoln v. Interlas*[31] the Dutch Supreme Court granted an injunction to restrain a Dutch company from infringing the claimant's trademarks not simply in the Netherlands, but in all other countries in which the Defendant carried on business. As the Dutch courts are fast, relatively inexpensive[32], used to dealing with evidence in English and applying foreign law, the Netherlands has become the jurisdiction of choice for claimants seeking injunctive relief in multiple jurisdictions[33]. In *Philips Electronics v Postech Princo*[34] which was an action between a Dutch company and Swiss and Taiwanese defendants, the Dutch Supreme Court held that the courts of the Netherlands have power to grant cross-border interim as well as final injunctions.

F. BLOCKING ORDERS

35. These are injunctions to restrain an Internet service provider (ISP) or other intermediary from allowing its services to be used to infringe copyright. More specifically, they require the intermediary to restrict their subscribers' access to websites distributing infringing material or, more recently, streaming services accessible through set-top boxes loaded with special software[35]. Blocking orders are discussed in detail in Part F of this study. Save for the first application for a blocking order, which was refused on the grounds that the relief sought was too wide and unnecessary in view of the relief already granted[36], blocking orders are made almost as a matter of course in England and Wales. The defendants, who tend to be ISPs, rarely defend them. The parties affected by them[37] have every incentive not to come before the courts. To a large extent the court acts administratively rather than judicially when considering applications for blocking orders. In Denmark, Italy, Portugal and Lithuania, blocking orders are made by the executive rather than the judiciary. However, even in those countries there is an initiating or supervisory role for the courts.

---

29 *Twentieth Century Fox Film Corporation and others v British Telecommunications Plc* [2011] EWHC 2714 (Ch), [2012] Bus LR 1525, [2012] 1 All ER 869.

30 527 U.S. 308 (1999) (https://supreme.justia.com/cases/federal/us/527/308/).

31 HR 24-11-1989, NJ 1992/404.

32 According to TaylorWessing's Patent Map a patent infringement action can cost anything from £200,000 to £1 million in England and Wales but only €75,000 to €200,000 in the Netherlands (https://united-kingdom.taylorwessing.com/patentmap).

33 Wouter Pors (2004), *Philips Electronics v Postech Princo* May 2004 Bird & Bird (https://www.twobirds.com/en/news/articles/2004/philips-electronics-v-postech-princo).

34 *Ibid.*

35 *The Football Association Premier League Ltd v British Telecommunications Plc and others* [2017] EWHC 480 (Ch), [2017] ECC 17.

36 *Twentieth Century Fox Film Corporation and another v Newzbin Ltd* 2011] Bus LR D49, [2010] FSR 21, [2010] EMLR 17, [2010] EWHC 608 (Ch), [2010] ECC 13, [2010] ECDR 8.

37 Distributors of infringing matter and subscribers wishing to access such matter.

G. SMALL CLAIMS AND INTERNET COURTS

36. Not every content owner is a mighty broadcaster, publisher, film studio or record company. Individuals and small businesses also find that their photographs, videos, contract terms, sound recordings and other materials are reproduced without permission or even attribution. Because litigation is expensive and uncertain, most copyright holders prefer to endure the infringement than go to law. However, innovative court procedures can enhance access to justice and judicial efficiency. Three special internet courts have been established in China to deal with copyright disputes as well as other actions that arise from the use of the internet[38]. Unless otherwise ordered, the entire trial process takes place online, with more flexible procedures and rules of evidence. The first Internet court opened in Hangzhou where Alibaba is based. According to the China Daily, it handled over 10,000 cases in its first year[39]. The Hangzhou court proved to be so successful that two more have been opened, one in Beijing where Baidu is located and the other in Guangzhou where Tencent has its head office[40].

37. There is already a small claims track court in England for IP infringement claims other than patent, registered and registered Community designs, semiconductor topography and plant variety cases under £10,000 that can be decided in one day and where recoverable costs are limited to loss of earnings, travel expenses, issue fees and £260 for counsel or solicitors' fees where an injunction is sought. Its caseload is growing, but it is nothing like the volume of work handled by the Chinese internet courts.

38. There are pending proposals to establish a Copyright Claims Board within the US Copyright Office with jurisdiction to award damages of up to $30,000 for copyright infringement[41].

IV. INDIRECT JUDICIAL MEASURES AND VOLUNTARY SCHEMES

39. The enforcement of copyright is moving away from court procedures to the application of voluntary measures by intermediaries[42]. A range of administrative and technical measures geared towards online copyright infringement have been developed to cope with the volume and velocity of infringements. These measures are often based on some form of notice to an intermediary and are applied in accordance with statutory provisions or voluntary codes.

---

38 See: Zhou Yuhang (2018) *Judicial Interpretations of Provisions of the Supreme People's Court on Several Issues Concerning the Hearing of Cases by Internet Courts* 11 Tsinghua China L. Rev. 175.

39 *China first internet court handles over 10,000 cases,* 18 August 2019, ChinaDaily.com.cn (http://www.chinadaily.com.cn/a/201808/18/WS5b77c8f4a310add14f386801.html).

40 Meng Yu and Guodong Du (2018), *China Establishes Three Internet Courts to Try Internet-Related Cases Online* 16 Dec 2018, China Justice Observer (https://www.chinajusticeobserver.com/insights/china-establishes-three-internet-courts-to-try-internet-related-cases-online.html).

41 Identical Bills H.R.2426 and S.1273 *Copyright Alternative in Small-Claims Enforcement Act of 2019* (*the CASE Act of 2019*) were introduced in the US House of Representatives and Senate on May 1, 2019, to establish a Copyright Claims Board " as an alternative forum in which parties may voluntarily seek to resolve certain copyright claims regarding any category of copyrighted work". See: Lambert (2019), *A Small Claims Tribunal for Copyright Cases in the USA* 17 Jan 2019 NIPC News (https://nipcnews.blogspotcom/2019/01/a-small-claims-tribunal-for-copyright.html).

42 Bernt Hugenholtz (2010), *Codes of Conduct and Copyright Enforcement in Cyberspace*, in Irini A. Stamatoudi (2010), *Copyright Enforcement and the Internet*, Kluwer Law, at pp 303–320. See also in general Kate Klonick and Thomas Kadri (2018), *How to make Facebook's "Supreme Court" work*, New York Times, 17 November 2018.

A. NOTICE AND TAKEDOWN

40. "Notice and takedown" is an administrative and technical procedure. It requires intermediaries to remove infringing content online, upon notice by copyright holders. Notice and takedown is one of the most-used measures to combat the infringement of intellectual property rights online. It was first developed in response to copyright infringements[43]. The notice and takedown procedure was originally developed in the US as part of the Digital Millennium Copyright Act (DMCA)[44]. The Act also offers protection to ISPs in the form of 'safe harbor' provisions[45]. The legal basis for notice and takedown procedures in the EU is Article 14 of Directive 2000/31/EC on Electronic Commerce. This creates the obligation of online hosts to actively remove or disable access to infringing content once they are made aware of it, i.e. receive notification by the rights holder. However, the provision only provides a basis and does not specify how notice and takedown procedures work in practice. At the time the directive was enacted, it was hoped that initiatives would be developed and that member states would have the freedom to form their own notice procedures[46].

41. The legal uncertainty of a host's obligations in reality under Article 14 is problematic for several reasons. There have been volumes of litigation at a national level and numerous referrals to the European Court of Justice. Clarification is needed and this might best be achieved through the development of a guide on the matter, applicable across all member states. The European Commission has made attempts at this by publishing a consultation in 2010[47], which addressed the limitations of the Directive and suggested measures to reform the current regime[48].

42. Although there have been a significant number of successful takedowns[49] as well as many of the largest platforms implementing a notice and takedown framework, notably Alibaba[50] and Google[51], the effectiveness of the measure has often been called into question. Doubts have been cast over the ability of notice and takedown to adequately protect right holders rights, the risk of taking down non-infringing content, including authorized content and the persistence of the whack-a-mole problem – (where a webpage is taken down, another online listing usually pops up under a different URL almost instantly as the infringers themselves evade identification[52]).

---

43 A. Marsoof (2016), Holding Internet Intermediaries Accountable for Infringements of Trademark Rights: Approaches and Challenges' (PhD Thesis, King's College, London).

44 Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860.

45 17 U.S.C. §512.

46 It should be noted that in accordance with the new Article 17 of the EU Directive on Copyright in the Digital Single Market, platforms have to maintain effective notice-and-takedown mechanisms based on the information provided by copyright holders – see for example Finland, Lithuania and Poland's adoption of notice and takedown procedures https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2575069.

47 European Commission (2010), *The future of electronic commerce in the Internal Market and the Implementation of the Directive on Electronic Commerce*.

48 In 2012, the European Commission announced a new initiative, which focused entirely on Notice and Action procedures (Commission Communication, *A coherent framework for building trust in the Digital Single Market for e-commerce and online services*, (2012)). The initiative's aim was to create a Europe-wide framework to deal with illegal content online, covering the challenges of implementing procedures and maintaining a proportional approach in doing so. A response to the consultation was expected in 2013. Although a Staff Working Document was published (Commission Staff Working Document, 'E-commerce Action plan 2012-2015 – State of Play 2013'), no further guidance was provided and the next steps on Notice and Action procedures are to be awaited (Aleksandra Kuczerawy, "Intermediary Liability & Freedom of expression: Recent developments in the EU Notice & Action Initiative" (2015).

49 Alibaba Group, Re: 2016 Special 301 Out-of–Cycle Review of Notorious Markets.

50 Ni Liang (2014), *Intellectual Property Protection Practices of Alibaba Group under the Internet Platform-Based Business Model*.

51 Now Google Fights Piracy report - https://www.blog.google/outreach-initiatives/public-policy/protecting-what-we-love-about-internet-our-efforts-stop-online-piracy/).

52 Frederick Mostert (2017), *Study on Approaches to Online Trademark Infringements*, WIPO/ACE/12/9 REV. 2.

43. Urban, Karagani and Schofield demonstrate that a major concern with the notice and takedown procedure is the potential of over-blocking or taking down material which is not infringing copyright[53]. In addition to mistaken notices, some notices are sent in bad faith to "silence commentary or unwanted criticism"[54], and to disrupt the legitimate business practices of competitors. Facebook has been criticized for its content removal process. The Electronic Frontier Foundation (EFF) has asserted that for many Facebook users, the content that the social media platform has removed in error has not been restored and that in some cases users were banned from the platform, without justification[55]. Notice and takedown is susceptible to misuse. There is a significant issue in that over-blocking could have a chilling effect on free speech by pre-emptively removing content which does not infringe copyright[56]. Although counter-claims, introduced to remedy incorrect takedowns, are available, studies show that they are rarely used in practice[57].

44. Another limitation to notice and takedown measures is that online pirates are developing their competency with technical tools at an increasing rate. For instance, once a page has been taken down, pirates have the tools to restore pages by, for example using a new location. This leads to an endless game of whack-a-mole[58], whereby once one website is taken down, many others pop up, sometimes just minutes later. This problem is not confined to copyright and is arguably even more acutely the case with trademark infringement[59].

45. "Robo-takedowns" have taken off in light of the volume of infringing material and the whack-a-mole problem. "Robo-takedowns" are automated takedown requests directed to ISPs. Such takedowns are based on algorithmic tools which are deployed to surveil the Internet to pinpoint infringing material[60]. Carpou argues that in light of the number of takedown requests received[61], automated processes such as robo-takedowns are the most efficient way for ISPs to tackle the volume of requests[62].

46. However, there have also been concerns over the accuracy of automated systems. Carpou suggests that "at least in some instances, robo-takedown requests have a chilling effect on free speech by preemptively removing content that does not violate anyone's copyright"[63]. According to Urban, Karaganis & Schofield, about 30% of automated copyright takedown requests failed accurately to identify allegedly infringed works or material[64]. These processes

---

53 Approximately 30% of notice and take down requests are made in error according to a study by the University of California, Berkeley, and Columbia University: Jennifer Urban, Joe Karagnis and Brianna Schofield (2017), *Notice and Takedown in Everyday Practice*, UC Berkeley Public Law Research Paper No. 2755628. Available at SSRN: https://ssrn.com/abstract=2755628.

54 Devlin Hartline (2016), *Why Notice-and-Staydown Just Makes* Sense, accessible at https://cpip.gmu.edu/2016/01/14/endless-whack-a-mole-why-notice-and-staydown-just-makes-sense/.

55 https://www.eff.org/press/releases/eff-human-rights-watch-and-over-70-civil-society-groups-ask-mark-zuckerberg-provide.

56 Zoe Carpou (2016), *Robots, Pirates, and the Rise of the Automated Takedown Regime: Using the DMCA to Fight Piracy and Protect End-Users*, 39 Colum. J.L. & Arts 551, at 554; Wendy Seltzer (2010), *Free Speech Unmoored in Copyright's Safe Habour: Chilling Effects of the DMCA on the First Amendment*, Harvard Journal of Law & Technology, Vol. 24, p. 171, 2010; Berkman Center Research Publication No. 2010-3. Available at SSRN: https://ssrn.com/abstract=1577785.

57 Jennifer Urban, Joe Karagnis and Brianna Schofield (2017), footnote 53 above.

58 Frederick Mostert (2019), *Digital Tools of Intellectual Property Enforcement – their intended and unintended norm-setting* consequences, chapter in *Research Handbook on IP and Digital Technologies*, edited by Tanya Aplin (in press 2019).

59 Frederick Mostert (2017), footnote 52 above.

60 Zoe Carpou (2016), footnote 56 above.

61 Google reported that its search engine received requests to take down over 63 million URLs in the month of December 2015 (Transparency report).

62 Zoe Carpou (2016), footnote 56 above.

63 Zoe Carpou (2016), footnote 56 above.

64 Jennifer Urban, Joe Karagnis and Brianna Schofield (2017), footnote 53 above. *See also: Evan Engstrom and Nick Feamster (2017), the Limits of Filtering: A Look at the Functionality and Shortcomings of Content Detection Tools, accessible at https://www.engine.is/the-limits-of-filtering.*

operate on a largely automated procedure, without human overview or intervention to verify alleged infringing content. Accordingly, efficiency may operate at the price of accuracy.

47. Some e-commerce companies have sought to fill this gap by developing their own clear notice and takedown procedures. For example, Alibaba reports that it has implemented a notice and takedown program for potential copyright, trademark, design and patent infringement[65]. Alibaba has also sought to develop simple, transparent notice and takedown procedures and a "one-stop-shop Intellectual Property Platform where rights holders may register to enforce their IP rights across all Alibaba platforms"[66].

48. Few e-commerce platforms consistently report notice and takedown statistics, but the statistics that are available are encouraging. For example, Alibaba reports that, between September 2017 and August 2018, the number of takedown requests on Alibaba platforms decreased 44 per cent, while participation on Alibaba platforms increased 36 per cent[67].

B. NOTICE AND STAYDOWN

49. Notice and stay down is a measure which developed in part due to the volume of online infringements and the whack-a-mole problem mentioned above. Notice and stay down is based on ISPs taking down infringing content followed by monitoring their digital space for the same infringing content. ISPs need to identify any reoccurrence of the content (or Bad Actor) on their platform and block it again, with the aim of preventing it from reappearing and making sure it "stays down"[68]. Proposals for the introduction for notice and stay down rules have been made in the US[69] and in the EU[70].

50. The United Kingdom Intellectual Property Office (UKIPO) has outlined a strategy for enforcement by taking a stronger stance towards copyright, trademark and patent infringement in the UK between now and 2020[71]. The UK government is also considering an "administrative website blocking" procedure[72].

---

65 Alibaba's Submission for the 2017 Special 301 Out-of-Cycle Review of Notorious Markets ("Alibaba's 2017 Special 301 Submission"), Part II, at 11 and Appendix 3.

66 Alibaba's Submission for the 2018 Special 301 Out-of-Cycle Review of Notorious Markets ("Alibaba's 2018 Special 301 Submission") at 8.
Alibaba's 2018 Special 301 Submission at 7. Alibaba reports that, in 2018, Alibaba's Taobao Marketplaces handled 97% of all takedown requests (including but not limited to submissions under Alibaba's good faith program) within 24 hours during business days.

67 Alibaba's 2018 Special 301 Submission at 4 and 6. This would imply that the number of infringements appearing on the Alibaba platforms is declining. However, the decline may be due to a number of different IP protection programs Alibaba has employed in addition to traditional notice and takedown. For example, Alibaba has stated that it seeks to identify problematic listings proactively (without a notice from a rights holder). It reports that, between September 2017 and August 2018, it took down 23 times more listings proactively than through its notice and takedown process, and "97 per cent of those proactive takedowns were removed before a single sale took place." These types of actions imply that the availability of a notice and takedown safe harbor does not create a perverse incentive for ISP's to avoid implementing programs to police their listings for infringing material. See: Alibaba's Submission for the 2016 Special 301 Out-of–Cycle Review of Notorious Markets; Alibaba's 2017 Special 301 Submission at 15-21; and Alibaba's 2018 Special 301 Submission at 6-10.

68 Frederick Mostert (2017), footnote 52 above.

69 https://blog.archive.org/2016/06/02/copyright-offices-proposed-notice-and-staydown-system-would-force-the-internet-archive-and-other-platforms-to-censor-the-web/.

70 Article 17 of the EU Directive on Copyright in the Digital Single Market.
It should be noted that in accordance with the new Article 17 of the EU Directive on Copyright in the Digital Single Market, platforms now have to maintain effective notice-and-stay-down mechanisms based on the information provided by copyright holders.

71 The Intellectual Property Office (2016), *Protecting creativity, supporting innovation: IP enforcement 2020*.

72 The Intellectual Property Office (2018), UK Government response to the call for views regarding illicit IPTV streaming devices. See also: https://www.pinsentmasons.com/out-law/news/uk-out-of-court-website-blocking-considered.

51. Platforms, in practice, will use automatic filtering recognition proactively to monitor their content for reoccurring infringements. Notably, YouTube has developed a Content ID system, which involves working with copyright owners to assist the identification of illegal content on their platform[73]. Similar technology, using digital fingerprinting to facilitate the filtering function of notice and stay down procedures, has also been developed by Audible Magic[74] (used by platforms such as Facebook and Soundcloud).

52. However, the development of such filtering systems is cause for concern over the cost required for platforms[75]. In addition, it is difficult to set up a filtering system that will work across the board for all platforms[76]. For example, YouTube has spent $100 million developing its Content ID[77]. On a related note, the issue of costs was at the heart of the *Cartier*[78] trade mark case, where the UK Supreme Court decided that the costs of implementing a blocking order should be assumed by the right holder.

53. The use of notice and stay down has attracted support[79] which is demonstrated through the institutional response to the concept. For example, the European Commission has given its endorsement in a Communication published last year[80]. German courts have demonstrated support for the concept of notice and stay down, as evidenced in the Rapidshare case[81].

54. However, the French Cour de Cassation has held that a judge-imposed requirement to prevent the reappearance of content that has already been removed would be equivalent to imposing a type of general monitoring obligation, contrary to Article 15 of the E-Commerce Directive[82]. Additionally, the Court of Justice of the European Union (CJEU) has held that a general monitoring obligation constitutes a disproportionate interference with the intermediaries' and users' fundamental rights[83].

55. Issues which have surfaced in respect of notice and stay down procedures are as follows:

- It is difficult to implement a notice and stay down procedure so as to strike a proportionate balance with fundamental rights[84];

---

73 https://www.virgin.com/music/how-are-youtube-and-google-fighting-piracy. Videos uploaded to YouTube are scanned against a database of files which have been submitted to the platform by content owners. When YouTube matches a work they own, copyright owners can decide what happens to the content. For example, they can allow, monetize or block the content.

74 Audible Magic was one of the first commercial fingerprinting and filtering services for audio and enjoyed active promotion by the Recording Industry Association of America ("RIAA") as early as 2004. See: Jennifer Urban, Joe Karagnis and Brianna Schofield (2017), footnote 53 above, at page 58.

75 Jennifer Urban, Joe Karagnis and Brianna Schofield (2017), footnote 53 above.

76 https://blog.archive.org/2016/06/02/copyright-offices-proposed-notice-and-staydown-system-would-force-the-internet-archive-and-other-platforms-to-censor-the-web/.

77 https://venturebeat.com/2018/11/07/youtube-weve-invested-100-million-in-content-id-and-paid-over-3-billion-to-rightsholders/.

78 *Cartier International AG & Ors v British Telecommunications Plc & Anor* [2018] UKSC 28 (13 June 2018).

79 Devlin Hartline (2016), footnote 54 above.

80 European Commission (2017), *Tackling Illegal Content Online, towards an enhanced responsibility of online platforms* (Communication) COM (2017).

81 *GEMA v RapidShare* I ZR 79/12 (Bundesgerichtshof, August 15, 2013).

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

83 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM).,* C-70/10, EU:C:2011:771.

84 Frederick Mostert (2017), footnote 52 above.

- As with notice and takedown, freedom of speech and access to information may be compromised, especially where lawful content is taken down[85];
- Where notice and stay down involves systematic analysis of information, it could represent a "disproportionate interference" with data protection rights[86];
- Some say it would be a filter everything approach[87] - there would be a burden on platforms to monitor user activity constantly;
- Will there be sufficient judicial review of fundamental rights at stake when either private platforms or government authorities are in control of the notice and stay down process?

C. NOTICE AND NOTICE

56. In some jurisdictions, ISPs have a responsibility either under the law or by voluntary agreement with right holders to forward notices of suspected infringement to internet account holders. However, the aim of such systems is primarily educational. No contractual or judicial consequence necessarily follows from the receipt of multiple notifications. Examples of this type of regime are found in Canada, Chile, Costa Rica and the UK[88].

D. FILTERING AND MONITORING

57. Filtering and monitoring for illegal copyright content especially by Big Tech players such as YouTube, Facebook and Instagram have become almost standard. Such filtering and monitoring by tracing and matching digital fingerprinting of unique identifying hashes of digital copyright files have in effect become the new norm in the industry. The Big Tech players, however, are armed with significant financial and IT resources which enable them to more effectively weed out infringing content on their curated platforms. ISPs which are start-ups or SMEs, on the other hand, may not easily have access to the requisite financial or IT resources to implement the same type of filtering or monitoring[89]. This state of affairs no doubt presents a potential competition law issue for new entrants into the platform markets.

---

85 Frederick Mostert, *ibid*.

86 Christina Angelopoulos (2016), *Notice-and-Fair-Balance: How to Reach a Compromise between Fundamental Rights in European Intermediary Liability*.

87 Elliot Harmon (2016), *Notice and Stay Down is Really Filter Everything*, Electronic Frontier Foundation.

88 In Canada, for example, under section 41 of the Copyright Act a copyright owner who detects an apparent infringement on the internet may send a notice (providing certain statutory particulars) to the service provider, who must then forward it to "the person to whom the electronic location identified by the location data specified in the notice belongs" – i.e., the account holder (See sections 41.25 and 41.26, R.S.C., 1985, c. C-42, as amended). Similarly, the law in Chile was amended in 2010 to provide for a "notice-and-notice" scheme - see Article 85U, Law No. 17.336 on Intellectual Property (as amended in 2010). In 2011, Costa Rica made similar provision (See Regulation on the limitation of liability of service providers for infringement of Copyright and Related Rights in accordance with Article 15.11.27 of the Free Trade Agreement Dominican Republic-Central America-United States (2011). Certain purely voluntary schemes are to similar effect. In the United States, a voluntary notice-and-notice scheme operated from 2011 under the auspices of the Center for Copyright Information, pursuant to a multilateral agreement between a number of leading ISPs and trade associations representing the copyright industries. However, the scheme ceased to operate in late 2016. A similar voluntary scheme, *Creative Content UK*, was announced in the UK in 2014 as part of a wider piracy reduction strategy, with substantial financial support from the UK Government (UK Government press release, July 19, 2014, *New education programme launched to combat online piracy* (https://www.gov.uk/government/news/new-education-programme-launched-to-combat-online-piracy)).

89 A refreshingly proportionate view on smaller companies' duties is taken in the UK Government, DCMS Online Harms White Paper, 8 April 2019, at 88 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

58. Until recently, EU law was also predicated on the premise that no "general monitoring obligation" should be imposed on platforms to eliminate infringing copyright material in accordance with Article 15 of the E-Commerce Directive and the CJEU's decision in Sabam/Netlog[90]. The new Article 17 of the EU Directive on Copyright in the Digital Single Market[91] has changed all of this now, in effect, requiring a "general monitoring obligation" of platforms and 'online content sharing service providers' (OCSSP) notably YouTube and Facebook.

59. Article 17 effectively introduces strict, primary copyright infringement liability for online user-generated content platforms[92]. Some commentators such as Professor Senftleben argue that this new strict liability of platforms for infringing content places a heavy burden on them[93]. Also, critics have called the directive a "censorship machine" that would harm free speech, impose new obligations on platforms that would be technically impossible for them to comply with, kill memes and GIFs[94].

60. In future, platforms may in these new circumstances no longer be able to rely on "safe harbor" provisions and the importance of specific "knowledge" of infringing content may not be so determinative[95]. Platforms will, in accordance with Article 17, now have to show that they have made "best efforts" to obtain a license or authorization from the copyright holder (for films, music, books and other works). And, in cases where the platforms do not obtain such authorization, they have to filter and pre-emptively block "specific works" – on which the copyright holders have provided "the relevant and necessary information" such as the digital fingerprints or id hashes of the works in question. As Professor Visser notes, YouTube and Facebook already carry out a fair amount of filtering at the request of the film and music industry – but they may have to do more[96]. In addition, platforms have to maintain effective notice-and-takedown and notice-and-stay-down mechanisms based on the information provided by copyright holders and must provide for effective and expeditious complaint and redress mechanisms.

61. It should be noted, that in view of the competition law concerns outlined above on market entry by start-up and SME platforms, Article 17 provides an exemption for those platforms which have operated for less than three years and have a turnover of below EUR 10 million. These platforms do not have filter and blocking obligations.

62. It is inevitable that disputes will continue unabated over the removal of disputed works on platforms. In this context, Article 17, most interestingly, requires that removals shall be subject to "human review". Human analysis is even more relevant in the context of preventing overblocking in relation to works of satire, parody, pastiche and other highly nuanced works. By introducing these provisions, an effort is made to strike a balance between freedom of

---

90 *Sabam v Netlog NV*, Case C-360/10.

91 Accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1563293899592&uri=CELEX:32019L0789. It should be noted that the Directive only covers "online content sharing service providers" and online marketplaces and sharing platforms are, for example, specifically excluded. It will be of interest to see how the reach and scope of Article 17 will be interpreted and implemented by the courts in Europe and ultimately the EUCJ.

92 Dirk Visser (2019), *Trying to Understand Article 13* at 4, SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3354494).

93 Martin Senftleben (2019), *Bermuda Triangle – Licensing, Filtering and Privileging User-Generated Content Under The New Directive on Copyright in the Digital Single Market*, SRRN at 17: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3367219).

94 Eleonora Rosati (2019), *The EU's New Copyright Laws Won't 'Wreck the Internet'*, at 2, SSRN, https://slate.com/technology/2019/04/eu-copyright-directive-article-13-wreck-internet.html).

95 It is of interest to note that the UK Government in its new White Paper proposal on internet regulation has also deviated from a general monitoring obligation in certain circumstances - in cases of national security and child sexual exploitation and abuse online. See UK Government, DCMS Online Harms White Paper, 8 April 2019, at 43 and 63 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

96 Dirk Visser (2019), footnote 92 above.

expression and freedom of the arts on the one hand and intellectual property rights on the other. On the flipside of the coin though, it may be argued that the volume and velocity of disputed works on platforms cannot conceivably all be analyzed and reviewed by humans. It remains to be seen how this provision will play out in practice.

63. Critics also express the concern that filtering is a drastic measure which may involve making critical decisions about underlying fundamental rights including free speech. As Dr. Angelopoulos demonstrates, the potential of filtering having a "chilling effect" on free speech is present and real[97]. Filtering, it is submitted, may require judicial legal review in some instances rather than representing a stand-alone, private regulatory function[98].

64. Platforms need to ensure effective and expeditious complaint and redress mechanisms for users who generate content as echoed in Article 17. Moreover, the process of review and moderation of content by platforms needs to be transparent.

> "For example, with a large volume of decisions surrounding content moderation now being fully or partly automated there is a risk that decision-making takes place within what Professor Frank Pasquale calls "the black box", a system whose workings are mysterious; only inputs and outputs can be observed, but not the process in between"[99].

65. . Concern has also been voiced about the lack of easy-to-access complaint mechanisms across the board for users to rely on cases of unjustified blocking by platforms. More rigorous, uniform and user-friendly complaint mechanisms are required together with an appropriate appeals function. Complaints also need to be responded to and processed within a reasonable timeframe[100].

---

97 Christina Angelopoulos (2019)**,** *Should Article 13 be amended?*, http://copyrightblog.kluweriplaw.com/2018/06/29/axel-vosss-juri-report-article-13-violate-internet-users-fundamental-rights/. Conscious of this concern in a related context, the UK Government in its White Paper on Online Harms UK Government, footnote 89, at 56 notes that "The regulator … will ensure that the new regulatory requirements do not lead to a disproportionately risk averse response from companies that unduly limits freedom of expression …" Professor Keller (Daphne Keller (2019), "Who do You Sue, State and Platform Hybrid Power Over Online Speech, A Hoover Institute Essay", at 27, https://www.hoover.org/sites/default/files/research/docs/who-do-you-sue-state-and-platform-hybrid-power-over-online-speech_0.pdf) also points out that in the US users, who generate content online (such as parodies or criticisms), have had their works taken down by platforms as infringing copyrighted material with little redress. These users have often failed to compel the platforms to re-instate such content on the grounds of free or artistic expression. The users have argued that the platforms essentially act as public forums and therefore "must carry" their works or content (Keller refers to such cases as "must carry" claims, see Daphne Keller, above at 18). The argument which the platforms have wielded against such "must carry" claims by users, is a free speech defense. The defense is predicated on the premise that platforms, as private content curators, will lose the right to express their editorial judgement through their removal choices (Daphne Keller, above at 17. The counter- arguments from "must carry" claimants are that the Big Tech platforms, with large market shares, essentially have in reality become the gatekeepers of today's public forums. The platforms should, therefore, have special obligations or a duty of care towards users who generate speech and content on their platforms. Moreover, as Keller points out, major platforms are akin to monopolistic utility providers which provide the essential infrastructure for speech to be enabled online. Some also argue that platforms, which act as public forums, effectively stand in the shoes of the State and accordingly have to assume the State's duties towards its citizens. These are persuasive and compelling arguments on both sides of the divide.)

98 Platforms will no doubt be severely tempted to err on the side of caution and resort to over-blocking to avoid possible liability to content holders.

99 UK House of Lords (2019), Select Committee on Communications, *Regulating in a Digital World*, March 9, 2019, at 17 and 56 and 59, https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf.

100 See UK Government, DCMS Online Harms White Paper, April 8, 2019, at 8 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf. Some would argue as Article 17 implies a general monitoring obligation that goes against the principle of limited intermediary liability enshrined in Article 15 of the e-Commerce Directive and ECJ case law. Others argue that there are very serious, and perhaps insurmountable, technical difficulties with implementing this requirement of Article 17. The Directive might, for example, require platforms put in place upload filters to scan every piece of content uploaded or shared by users and check it against a database of copyrighted material. However, many platforms believe that the technology does not exist to create filters that could reliably distinguish between

66. It should be noted that some platforms such as Amazon have developed digital tools which provide rights holders with advanced capabilities to protect their content and other intellectual property on the platform. For example, Amazon's "Brand Registry" tool includes powerful text- and image-based search capabilities which can detect copyright infringement and automated protections that use machine learning to predict and prevent future defects. Right holders also receive greater influence over their detail pages – so they can ensure copyright and product information is accurate and customers can make confident, informed purchasing decisions[101].

E. LICENSING

67. Licensing and pre-clearance has been proposed as a possible way forward to limit online piracy. In other words, virtually all copyrighted works will need to be pre-cleared and licensed before they are uploaded to user-generated content platforms. This model is one of the cornerstones of Article 17 of the EU Directive on Copyright in the Digital Single Market.

68. As Dr. Rosati indicates, users might actually be better off than they are under the current system[102]: "For instance, if a platform secures a license in relation to certain content, users will cease being directly responsible for materials that they upload. The license will, in fact, cover both the platform and the user. This is a significant change… With this new provision, in some cases, it will be the platform that will bear the responsibility for the content you share, not you"[103].

---

legitimate and infringing content. If this is true, and given the threat of potential penalties and litigation for failure to comply with Article 17, platforms may err on the side of caution and remove content when there is any conceivable doubt about its legitimacy. Platforms of all sizes may face this challenge, but start-ups, in particular, might not be able to afford to dedicate the financial and human resources necessary to implement filtering technologies for user-generated content. The Directive may force them to take an overly broad approach in removing content, or they may simply abandon or shrink their business, which could have significant adverse consequences for innovation. Furthermore, removing vast amounts of legitimate content potentially could restrict freedom of speech and the right to receive information.

101 https://blog.aboutamazon.com/policy/protecting-customer-trust.

102 Eleonora Rosati (2019), footnote 94 above.

103 For platforms though, Article 17 "it creates a rights clearance task which (they) can hardly ever accomplish" (Martin Senftleben (2019), footnote 93 above). As Professor Senftleben illustrates: "An online content platform seeking to obtain a license for user generated content is thus confronted with an enormous licensing task. .. the license should ideally encompass the whole spectrum of potential posts." A fair amount of the devil is in the detail and solutions will have to be found in the practical applications of this new licensing framework. For instance, as pointed out, collecting societies would need to provide all-embracing licenses for the entire work in all EU member states (op. cit.). On the whole, the collecting society landscape is fragmented and few pan-European solutions are on offer. In effect, "EU citizens will no longer enjoy the freedom of uploading remixes and mash-ups of all kinds of pre-existing material…As a corollary … platforms will no longer offer the content diversity that is currently available. Hence, the licensing approach entails the risk of a substantial loss of freedom of expression and information… In the light of the EU's cultural diversity, the problem has a broader dimension: user generated content impoverishment entails the risk of neglecting minority groups, minority views and niche audiences" (op. cit.). The prediction is that, in view of the current content and collection infrastructure, for film, music, audio-visual works, literary and pictorial works, it will be hard to secure clearances (Dirk Visser (2019), footnote 92 above). Moreover, licensing in practice is being driven by business considerations and will most likely focus on the large film and music producers (the so-called Majors) in the larger EU countries. As noted, "the licensing option may thus bestow upon big players a competitive advantage that leads to further market concentration" (Martin Senftleben (2019), above, at 5), see also in a related context Christina Angelopoulos et al (2018), *The Copyright Directive: Misinformation and Independent Enquiry*, https://www.create.ac.uk/blog/2018/06/29/the-copyright-directive-misinformation-and-independent-enquiry/).

F. BLOCKING

69. Website blocking is a significant digital instrument in the toolkit to fight online piracy. It most commonly involves ISPs disabling access to certain websites which carry copyright infringing material. Such disabling can be implemented of their own accord by ISPs or on a request from right holders or industry trade associations within the framework of a voluntary scheme or otherwise. Blocking is often also effected by way of a court order in the form of an injunction at the request of the copyright holder. More recently, dynamic blocking, which goes beyond a specific website to include 'mirror sites', has proven to be successful[104].

70. Some assert that blocking is one of the most effective digital tools in fighting online copyright infringements[105]. For example, from experience in Denmark, visits to websites with infringing material were reduced by 75% within a short period of time after blocking[106]. Other commentators suggest that while blocking access to a broad spectrum of pirate sites is effective substantially to reduce visits to pirate sites, the positive effect on legitimate sales may diminish over time[107].

71. The use of website blocking orders is prevalent in the EU, where the possibility of granting such orders is made possible under Article 8(3) of the Information Society Directive[108]. Beyond Europe, several countries including Australia[109] and Singapore[110] have passed legislation to facilitate website blocking, and the first blocking orders in both countries were granted in 2016[111].

72. Denmark offers an example of the interplay between voluntary measures and judicial intervention. The first known judicial order to block a web site on grounds of copyright infringement was granted in Denmark in 2005. The RettighedsAlliancen is a Danish trade association working to promote a 'safe and sustainable online environment for both users and the creative businesses'[112]. In 2014, in the context of a dialogue initiated by the Danish Ministry of Culture, RettighedsAlliancen entered into a Code of Conduct (CoC) with Teleindustrien, the association representing major ISPs, with 85% of Danish Internet customers[113]. The only large nationwide ISP outside this association has also committed to apply the CoC. Under the CoC, when a court has found a particular web site to be infringing and ordered its blocking as against any particular ISP adhering to the CoC, all other ISPs will also block the site. Where a blocked site transfers to another domain, the ISPs will block that site if RettighedsAlliancen can show that only the domain name of the site has changed. Users who try to access a blocked site are directed to an online educational platform, *Share with Care*, directing users towards legal

---

104 RettighedAlliancen Report 2017, page 3: https://rettighedsalliancen.dk/wp-content/uploads/2018/05/ENGB_RettighedsAlliancen2018.pdf.

105 See above at footnote 104.

106 See Frederick Mostert (2019), at footnote 58.

107 Danaher, Brett and Smith, Michael D. and Telang, Rahul, Website Blocking Revisited: The Effect of the UK November 2014 Blocks on Consumer Behavior (April 18, 2016). Available at SSRN: https://ssrn.com/abstract=2766795.

108 Directive 2001/29 on the harmonization of certain aspects of copyright and related rights in the information society [2001] OJ L167/10.

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

110 Copyright Amendment (Singapore) Act 2014.

111 Sabesh Asokan (2018) *Demystifying the 'honest' infringer: reorientating our approach to online copyright infringement using behavioral economics*, Journal of Intellectual Property Law & Practice 737.

112 https://rettighedsalliancen.dk/forside-2/english/.

113 For a summary of the Code of Conduct (in Danish), see: http://www.teleindu.dk/wp-content/uploads/2014/10/TI-code-of-conduct-blokeringer.pdf.

sources of content. The Danish Government has recently undertaken to analyze the judicial process in the civil courts, to examine whether the procedure for blocking infringing web sites could be accelerated[114].

73. The use of website blocking by RettighedsAlliancen in Denmark has proved successful in fighting online piracy[115], with one blocking order resulting in a significant decrease in the number of visitors from Danish IP addresses[116]. In the beginning, RettighedsAlliancen used 'judicial-blocking': a process involving them to manually monitor visits to illegal websites and then requesting courts to label these as illegal. Telecoms companies could then block such illegal websites and instead provide a link to a 'Share With Care' platform, thus having the effect of 'directing' users away from illegal websites to legal ones. However, the legal framework for IP enforcement has been under discussion since 2017. RettighedsAlliancen has proposed that legislation be passed to allow the police to block illegal websites, obviating the requirement for civil actions[117].

74. In the first UK case of web site blocking, Mr. Justice Arnold held that there was jurisdiction to grant an injunction under section 97A of the Copyright, Patents and Designs Act 1988, which requires proof of knowledge on the part of the ISP that its services are being used for copyright infringement. British Telecommunications' service was being used to infringe copyright by the operators of the Newzbin2 website and its end users[118].

75. More recently[119], there has been another landmark case which saw the first UK 'live' blocking order in relation to streaming of content such as live sporting events[120]. In his judgment, Arnold J held that as a result of consumers using different ways to stream – via their IP addresses rather than websites – traditional blocking orders were no longer an appropriate remedy for rights holders[121]. This case shows the increased flexibility the courts are demonstrating when deciding cases in which technological advancements require a reconsideration of traditional approaches to copyright infringement[122]. There are proposals for "administrative blocking" of sites which carry copyright infringing content in the UK[123]. It is not clear whether such blocking will be subject to judicial review.

76. In Portugal, on the other hand, a Memorandum of Understanding was entered into in 2015 under the auspices of the General Inspectorate of Cultural Activities (Inspeção-geral das Atividades Culturais (IGAC)), between trade associations representing copyright owners, telecommunications operators and the advertising industry. Under this agreement, IGAC considers complaints of right holders that particular web sites are dedicated mainly to the infringement of copyright or related rights. The right holders must demonstrate that attempted without success to contact the operator of the web site to secure the removal of the infringing content. Where satisfied that a complaint is well-founded, IGAC issues a decision directing the blocking (by DNS blocking) of the site in question. This decision is then implemented by all the

---

114 Danish Ministry of Culture, May 2, 2019 *Growth Plan for the Creative Industries* (in Danish) (https://em.dk/media/13185/20456-em-vaekstplan-kreative-er-hverv-a4_web_enkeltsidet_04.pdf).

115 https://rettighedsalliancen.dk/forside-2/english/.

116 https://rettighedsalliancen.dk/forside-2/english/.

117 Annual Report 2017 – RettighedsAlliancen.

118 *Twentieth Century Fox Film Corp & Ors v British Telecommunications Plc* [2011] EWHC 1981 (Ch) (28 July 2011).

119 *FAPL v BT* [2017] EWHC 480 Ch.

120 *FAPL v BT* [2017] EWHC 480 Ch, para 11: consumers are increasingly turning to set-top boxes, media players and mobile device apps to access infringing streams, rather than web browsers running on computers.

121 *FAPL v BT* [2017] EWHC 480 Ch, para 11.

122 http://ipkitten.blogspot.com/2017/03/first-live-blocking-order-granted-in-uk.html.

123 See: UK Intellectual Property Office (2018), *UK Government response to the call for views regarding illicit IPTV streaming devices*, accessible at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/750177/Gov-Response-call-for-views-Illicit-IPTV.pdf; see also: https://www.pinsentmasons.com/out-law/news/uk-out-of-court-website-blocking-considered.

ISPs subject to the Memorandum of Understanding. The court is not involved, but the parties retain the right to have recourse to any judicial or administrative procedure to which they are entitled.

77. In Italy, the national Communications Authority (*Autorità per le Garanzie nelle Communicazioni* (AGCOM)) has operated an administrative system of site blocking since 2014[124]. AGCOM receives complaints by right holders through an online form. The operator of the web site is requested to remove the infringing content. If he fails to do so and offers no persuasive defense, AGCOM will direct the relevant hosting provider located in Italy to remove the specific content within three days. If satisfied that the web site is located outside Italy, AGCOM will direct Italian access providers to disable access to the infringing web site within three days. The decisions of AGCOM can be challenged in the Administrative Court of Latium. In case of non-compliance, AGCOM can impose fines of up to 250,000 euros.

78. Lithuania is in the process of adopting an administrative blocking procedure which includes ex-ante judicial confirmation[125].

79. Some commentators express the concern that blocking is a drastic measure which may involve making critical decisions about underlying fundamental rights, including free speech and privacy and should be subject to judicial review[126].

G. BAD ACTOR LISTING

80. Among the array of challenges that online piracy has produced is the sheer volume of pirates in the digital space. In addition, the task of identifying and tracking the pirates, with a view to removing unlawful content, can often involve Herculean efforts. To cope with these significant challenges, crucial systems of Bad Actor listing, redlisting, greenlisting and watch lists have developed. In a nutshell, these listings are “a central pivot in the work to monitor and fight cash flows and traffic” to sites or listings which carry illegal copyright content[127].

81. In particular, the use of Bad Actor listings to “follow-the-money” to the Bad Actors by collaborative efforts between law enforcement and platforms has had significant success in some jurisdictions. For example, the Bad Actor listing, also aptly called the “collaboration list” in Denmark, is a dynamic collection of illegal content services for films, series, music, literature, designs, live streaming and other pirated materials. Such Bad Actor listings are confidentially shared among law enforcement and government authorities as part of criminal investigations. Listings are used to identify and keep track of repeat offenders.

82. An example from the United Kingdom is Operation Creative and the Infringing Website List (IWL) of the City of London Police Cyber Crimes Unit (PIPCU). The aim of Operation Creative is to disrupt and prevent websites from providing unauthorized access to copyrighted content. The IWL is an online database containing a list of copyright infringing websites, which have been identified by the creative industries and verified by PIPCU. The aim of the IWL is that advertisers, agencies and other intermediaries can voluntarily decide to cease the placement of advertising on illegal content websites by using the data contained in the IWL. Such listing has the effect of disrupting advertising revenue from these sites[128].

---

124 Pursuant to Delibera n. 680/13/CONS del 12 dicembre 2013.

125 Article 78, Law No. VIII-1185 of May 18, 1999, on Copyright and Related Rights (as amended by Law No. XIII-1612 of November 28, 2018). https://www.e-tar.lt/portal/en/legalAct/TAR.551F0CDE5B64/asr.

126 See paragraphs 62 and 63 above.

127 RettighedsAlliancen Annual Report 2017, page 6: https://rettighedsalliancen.dk/wp-content/uploads/2018/05/ENGB_RettighedsAlliancen2018.pdf.

128 http://news.cityoflondon.police.uk/r/1184/pipcu_disrupts__719_million_worth_of_ip_crime.

83. The disruption of advertising is important and a key aim of Operation Creative because advertising is a significant generator of earnings for websites providing access to infringing content[129]. The appearance of advertisements, especially from established brands, on illegal websites suggests that those sites have a degree of legitimacy.

84. In a similar vein, RettighedsAlliancen in Denmark has developed the *"Disruption Machine"* which consists of a list of illegal content websites[130], which is shared with a network of participating stakeholders. Such stakeholders then ensure that the illegal websites do not receive advertisements, traffic or other sources generating cash flow. The idea is to hit the criminals behind these services most effectively – i.e., by targeting their revenues. Moreover, RettighedsAlliancen established a code of conduct, the "Kodex" under the auspices of the Danish Ministry of Culture, under which leading companies in the Danish media and marketing industries committed themselves not to permit the use of their services, including advertising services, for illegal purposes, such as to infringe intellectual property rights[131]. This code of conduct forms a basis for blocking advertisements to blacklisted sites.

85. As well as the use of such listing by state entities and law enforcement, some online platforms have voluntarily introduced redlisting to improve their own IP enforcement systems. Notably, Alibaba has employed big-data technology to scan all of its platforms, and accounts identified as creating fake storefronts to sell suspicious goods are redlisted and subjected to a range of contractual sanctions.

86. Greenlisting is used as a tool to help identify legitimate platforms and websites, by creating a database of trusted actors. In practice, this can be seen through a number of examples in relation to identifying authorized vendor sites, including Amazon, eBay and Alibaba.

87. There has also been a suggestion to implement an online listings classification system that allows a ranking of "lists" to be created depending on the nature of the infringer's activities[132]. Once developed, and as it increasingly becomes used by more and more law enforcement and governmental authorities and internet service providers, it could act as a global check and verification system.

H. COOPERATION WITH SEARCH ENGINES

88. An important method to ensure respect for copyright is through voluntary codes. There have been several efforts across the globe to introduce such codes as a framework for tackling the rise in online piracy. As Peter Yu has stated, "laws alone are insufficient, no matter how well they are enforced. These laws must be accompanied by a legal culture that fosters voluntary compliance"[133].

89. In February 2017, Google and Microsoft Bing joined a Voluntary Code of Practice, along with the Motion Picture Association, British Phonographic Industries Ltd, and other representatives of creative industries. This Code aims to determine the effectiveness of search

---

129 The two other ways that criminal gangs make money from digital piracy is subscription and malware. This is further discussed in Federation Against Copyright Theft (2017), *Cracking Down on Digital Piracy – Report*, at pages 9 – 11. Accessible at: https://www.fact-uk.org.uk/files/2017/09/Cracking-Down-on-Digital-Piracy-Report-Sept-2017.pdf.

130 This list currently consists of more than 1,600 illegal websites and is updated monthly.

131 http://adkodex.dk/kodex/.

132 See: Daria Chernysh (2019) *Blacklisting: A New Effective Digital Tool Against Counterfeit Sales Online*, LLM Dissertation, King's College London.

133 Peter K. Yu (2000) *From Pirates to Partner: Protecting Intellectual Property in China in the Twenty-First Century*. See also Sabesh Asokan (2018), footnote 111 above.

engines' voluntary measures to fight online piracy and to encourage industry collaboration. In addition, the Code provides for the facilitation of the removal of links to infringing content from the first page of internet search results[134].

90. Also, as stated in its progress report, Amazon has engaged with a number of industry groups in order to ensure that copyright infringements can be tackled such as the Alliance for Creativity and Entertainment (ACE), Union des Fabricants (UNIFAB), the Motion Picture Association (MPA), and the Automotive Anti-Counterfeiting Council (A2C2). Amazon has signed a Memorandum of Understanding with the International Anti-Counterfeiting Coalition (IACC), an industry organization that builds bridges between industries to protect IP rights[135]. As a result of Amazon's and IACC's collaboration, a program has been launched to identify opportunities for improvement and educate brands on Amazon's notice and takedown processes.

91. The UK Intellectual Property Office (UKIPO), in its 2016 report on the Government's intellectual property enforcement strategy plan for the next four years, pledged to 'work with search engines and social media platforms to actively reduce the availability of illegal content…'[136]. Three years on, there has been significant progress[137], in particular, the voluntary code between rights holders and search engine providers, Google and Bing[138]. However, there is still some way to go and, moving forward, the impact of changes made by search engines must be constantly assessed and monitored[139].

I. EVALUATING SELF-REGULATION

92. Compared to regulation by legislation, self-regulation arguably has some benefits. As Professor Hugenholtz points out, standards and norms set by private actors involved can be more specifically fine-tuned to the requirements of a specific industry sector[140]. This is especially the case in specialized sectors where government may have no or little knowledge[141]. Self-regulation means rules can be more readily updated. This flexibility feature[142] of self-regulation is more conducive to areas such as the internet, which are subject to continuous change[143]. Standards and norms developed by self-regulation are often less costly than the legal costs involved by going through the legislative process[144].

---

134 The "*Code of Practice on Search and Copyright*" came into force on 9 February 2017 and its objective is to lower down search results listings for websites which offer infringing content. https://www.lexology.com/library/detail.aspx?g=05ebdcb9-d13f-48c9-a879-864b2f933607. See also Giancarlo F Frosio (2018), *Why keep a dog and bark yourself? From intermediary liability to responsibility,* International Journal of Law and Information Technology, Volume 26, Issue 1, Spring 2018, Pages 1–33 (https://academic.oup.com/ijlit/article-abstract/26/1/1/4745804?redirectedFrom=fulltext).

135 https://brandservices.amazon.co.uk/progressreport; https://www.iacc.org/iacc-and-amazon-initiate-new-brand-engagement-program.

136 The UK Intellectual Property Office (2016) *Protecting creativity, supporting innovation: IP enforcement 2020*.

137 https://ipo.blog.gov.uk/2018/05/10/ip-enforcement-2020-two-years-on/.

138 See paragraph 88 above. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609478/code-of-practice-on-search-and-copyright.pdf.

139 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642324/IP_Crime_Report_2016_-_2017.pdf.

140 Bernt Hugenholtz (2010), *Codes of Conduct and Copyright Enforcement in Cyberspace*, in Irini A. Stamatoudi (2010), *Copyright Enforcement and the Internet*, Kluwer Law, at pp 303–320.

141 Bernt Hugenholtz (2010), footnote 139 above.

142 Monroe Price and Stefaan Verhulst (2000), *The Concept of Self-Regulation and the Internet*, in J. Waltermann & M. Machill (Eds.), *Protecting our children on the internet: Towards a new culture of responsibility* (pp. 133-198).

143 Bernt Hugenholtz (2010), footnote 139 above.

144 Bernt Hugenholtz (2010), footnote 139 above.

93. Self-regulation is not without issues. The ease of revision, as Professor Hugenholtz demonstrates[145], and non-binding features of self-regulation do not promote certainty. Self-regulation also is often less transparent than required[146]. In addition, self-regulatory codes could lead to costly litigation[147].

94. There are concerns self-regulation may result in "shadow" guidelines which are not inclusive of all stakeholders[148]. Typically, self-regulatory guidelines are set up by the industry parties most closely involved and do not take into account the public interest at large and in particular, consumers and web users[149]. Such norm-setting without accountability is a concern[150]. Therefore, it is even more crucial that public authorities are involved in the fight against online piracy, for example, bodies such as PIPCU.

J. THE POTENTIAL OF BLOCKCHAIN

95. Copyright infringement and enforcement in the context of the internet presents new and complex threats and challenges and thus requires novel mechanisms to deal with them. The answer[151] may lie in a range of digital tools, in particular, authentication tools such as blockchain and search engine delisting.

96. Blockchain has been identified as a "technical tool" which, along with, but not limited to, redlisting, notice actions and domain name tools, has the potential to fight intellectual property infringement in the digital space[152]. One of the advantages of using a decentralized ledger has been cited as relatively low costs regarding maintenance of such a database and the security and transparency of the process used to track the dissemination of copyright works online[153].

97. Blockchain can be most simply understood as a digital ledger consisting of transactions and data which are grouped into blocks, which are then linked into chains. The data inputted into the blocks are immutable – and cannot be modified or deleted retroactively. This immutable feature of the technology is one of the reasons it is so attractive from a security perspective, as well as facilitating authentication and authorization of data and transactions. There are a number of features of the functions and processes of blockchain technology which make it uniquely suited to face the challenges of copyright enforcement in the digital space[154].

98. Blockchain technology has the potential to evidence ownership rights. Such evidence is enabled by ledgers which create time-stamped records of data which are immutable. Such records evidence when certain content was first created. This is particularly useful in the context of unregistered intellectual property rights such as copyright. Such data records can provide evidence of the copyright work's "conception, use, qualification requirements and

---

145 Bernt Hugenholtz (2010), footnote 139 above.

146 Bert-Jaap Koops et al (2006), Should Self-Regulation Be the Starting Point? 124, in B-J. Koops, M. Lips, C. Prins, & M. Schellekens (Eds.), *Starting Points for ICT Regulation* (pp. 109-151). (IT & Law; No. 9). The Hague: T.M.C. Asser Press.

147 Bernt Hugenholtz (2010), footnote 139 above, at page 307.

148 https://www.eff.org/issues/shadow-regulation.

149 Bernt Hugenholtz (2010), footnote 139 above.

150 Bernt Hugenholtz (2010), footnote 139 above, at page 307.

151 Google has removed 4 billion URLs from its index.

152 Frederick Mostert (2019), footnote 52 above.

153 Hiroshi Sheraton (2017) *Blockchain and IP: crystal ball-gazing or real opportunity?* PLC Mag., 28(9), 41.

154 See further discussion of the functions of Blockchain which make it desirable for intellectual property purposes: Frederick Mostert, Jue Wang (2018), *The Application and Challenges of Blockchain in Intellectual Property Driven Businesses in China* 11 Tsinghua China L. Rev. 13.

status" [155]. By establishing ownership at the outset (first in time, first in right), copyright holders are enabled to protect their rights[156].

99. China is said to be at the forefront of harnessing the potential of the application of blockchain for intellectual property enforcement, evidenced by acceptance by the Hangzhou Internet Court of Blockchain-authenticated evidence in a copyright infringement case[157]. Furthermore, the Guangzhou Arbitration Commission issued its first ruling based on an "arbitration chain" in March 2018[158], one of the first of decisions making use of blockchain in this way. The decision confirms that the practice of providing transparent and traceable data, via blockchain, is acceptable evidence. The decision also demonstrates the potential of accepting blockchain as credible evidence by the Chinese Court[159]. It should be noted that in the United States, a number of States have passed legislation recognizing data recorded on a blockchain as constituting admissible evidence[160]. The practical application of blockchain as evidence in litigation is making significant progress.

100. An important potential issue raised by blockchain in the intellectual property field is the problem of determining the relevant jurisdiction and concomitant governing law in a dispute[161]. Information contained on a blockchain is stored on nodes which are distributed around the world. Each transaction involving a copyright work can potentially be located in more than one jurisdiction. Such circumstances could easily lead to uncertainty as the the applicable law and jurisdiction[162]. On the flipside, blockchain might assist in other ways. The WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty required contracting parties to protect rights management information which was defined as "information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information"[163]. This information could be contained in a blockchain ledger.

V. CONCLUSION

101. Just as the nature of piracy is changing in light of the ever-expanding digital environment, so do the enforcement measures used to combat the threat. Effective guidance and tools used to fight digital piracy are still not in place. Traditional copyright enforcement mechanisms and the remedies for intellectual property rights infringement currently available are poorly adapted to deal with the fast-changing nature of copyright infringements online. Such mechanisms suffer from major limitations. These mechanisms also do not provide a suitable and proper basis for balancing underlying societal interests and fundamental rights.

102. *De facto* guidelines have already developed around the world with copyright holders, online and social media platforms, and government law enforcement authorities voluntarily cooperating across borders. These guidelines are in need of further evolution because the Internet is by its nature global. As anyone in charge of enforcement efforts will attest, the borderless digital environment and associated global jurisdictional issues make matters vastly

---

155 Birgit Clark (2018), *Blockchain and IP Law: A Match in Crypto Heavan?* WIPO Magazine, Februrary 2018 https://www.wipo.int/wipo_magazine/en/2018/01/article_0005.html.

156 Birgit Clark (2018), footnote 155 above.

157 https://www.sfgroup.hk/news_post/2575/.

158 *Ibid*.

159 Mostert, Wang (2018), footnote 154 above.

160 Ohio: OH SB220 (2017-2018); Arizona: AZ HB2603 (2018); Vermont: Act No. 157 (H.868) (2016).

161 John McKinley (2017) *Blockchain: background, challenges and legal issues* C.L.S. Rev., 33(5), 735.

162 https://www.dlapiper.com/en/uk/insights/publications/2017/06/blockchain-background-challenges-legal-issues/.

163 WIPO Copyright Treaty (WCT) (1996), Article 12(2); WIPO Performances and Phonograms Treaty (WPPT) (1996), Article 19(2).

challenging. In-depth research is urgently needed into the new principles of regulation which will necessarily result from the use of digital tools and administrative measures which are already paving the way for new legal standards throughout the world[164]. Effective enforcement in the digital environment can best be achieved through collaborative efforts on the part of copyright holders, content providers, and the public authorities, facilitated, where necessary, by uniform, voluntary guidelines.

[End of document]

[164] Frederick Mostert (2018), *The global digital enforcement of intellectual property* WIPO Magazine (https://www.wipo.int/wipo_magazine/en/2018/si/article_0005.html).