Faculty of Law

Research Paper No. 10/2020

Transnational Intellectual Property Governance on the Internet

Alexander Peukert [*]

Forthcoming in: Matthias Kettemann/Alexander Peukert (eds), The Law of Global Digitality

Proposed citation: Alexander Peukert, Transnational Intellectual Property Governance on the Internet, Research Paper of the Faculty of Law of the Goethe University Frankfurt/M. No. 10/2020, para.

Abstract: This article documents and classifies instances of transnational intellectual property (IP) enforcement and licensing on the Internet with a particular focus on the territorial reach of the respective regimes. Regarding IP enforcement, I show that the bulk of transnational or even global measures is adopted in the context of "voluntary" self-regulation by various intermediaries, namely domain name registrars, access and host providers, search engines, and advertising and payment services. Global IP licensing is, in contrast, less prevalent than one might expect. It is practically limited to freely accessible Open Content, whereas markets for fee-based services remain territorially fragmented. Overall, three layers of IP governance on the Internet can be distinguished. Based on global licenses, Open Content is freely accessible everywhere. Plain IP infringements are equally combatted on a worldwide scale. Territorial fragmentation persists, instead, in the market segment of fee-based services and in hard cases of conflicts of IP laws/rights. All three universal norms (global accessibility, global illegality, global fragmentation) are supported by a quite solid, "rough" global consensus.

[*] Dr. iur., Professor of Civil Law and Commercial Law, Faculty of Law, Goethe University Frankfurt am Main.

I. Introduction

1 Intellectual property (IP) is a classical cyberlaw topic and a prime example of the conflict between global online communication and local laws.[1] Whereas literary and artistic works, brands and other IP subject matter can, in principle, be made available to a global audience at virtually no cost via the Internet,[2] IP rights (IPRs) are strictly territorial in nature. International IP treaties make it possible to acquire 190+ local IPRs in, e.g. a motion picture or a well-known trademark, yet each local IPR is independent of all others and limited in its geographical scope to the territory of the IP jurisdiction granting it.[3] This fragmentation also bears on the rules of international jurisdiction and private international law.[4] IPRs requiring registration, such as patents, can be adjudicated in full only in the country of registration. Multistate copyright infringements may be decided by the courts in the defendant's domicile, but even these courts are bound to apply all IP laws of the states for which protection is sought.[5] Since pleading and applying 190+ copyright laws is unfeasible for both parties and courts, it has been proposed in the literature to reduce the number of laws applicable to ubiquitous online copyright infringements to one, namely the law of the closest connection with the (direct) infringement, and, regarding the indirect liability of Internet service providers (ISPs), the

---

[1] Cf Frank H Easterbrook, 'Cyberspace and the Law of the Horse' (1996) U Chi Legal F 207, 208 ("When asked to talk about 'Property in Cyberspace,' my immediate reaction was, 'Isn't this just the law of the horse?'"); Jane C Ginsburg, 'Global Use/Territorial Rights: Private International Law Questions of the Global Information Infrastructure' (1995) 42 J Copyright Soc'y USA 318. To be sure, the conflict between global commerce and local IPRs is also acute in offline settings; cf *Unwired Planet v Huawei* [2020] UKSC 37, 49-104 (allowing English courts to set global "FRAND" licensing conditions based on an alleged infringement of a standard-essential UK patent).

[2] *Google Inc v Equustek Solutions Inc* [2017] SCC 34, [2017] 1 SCR 824 ("The Internet has no borders — its natural habitat is global."). But see Dan Jerker B Svantesson, *Private International Law and the Internet* (2016) 57-8 (relative borderlessness of the Internet).

[3] Alexander Peukert, 'Territoriality and Extraterritoriality in Intellectual Property Law' in Günther Handl, Joachim Zekoll and Peer Zumbansen (eds), *Beyond Territoriality: Transnational Legal Authority in an Age of Globalization* (2012) 189-91.

[4] See Alexander Peukert in European Max Planck Group on Conflict of Laws in Intellectual Property (CLIP), *Conflict of Laws in Intellectual Property, The CLIP Principles and Commentary* (2013) paras PRE:C33-39.

[5] See, eg, *Boosey & Hawkes Music Publishers, Ltd v Walt Disney Co* [1998] 145 F3d 481, 491-2 (US court competent to adjudicate claim for damages for copyright infringement in at least eighteen foreign countries under these foreign laws).

law of the State of their center of business activity.[6] These proposals to overcome IP territoriality online have, however, not yet been taken up by any court or legislator.

2 It follows that a genuinely transnational governance of online IP activity necessitates "other rules" beyond formal IP laws, and the involvement of non-state actors.[7] IP rules that become transnational when they are implemented across borders. At a minimum, they affect two IP jurisdictions, at the most the entire Internet and thus global communication. The purpose of this article is to document and classify instances of such transnational IP "laws" of Western European and North American origin, with a particular focus on the territorial reach of the respective regimes.[8] It is structured according to the two basic options an IPR holder has available: She can either prohibit or authorize the use of her IP.[9] The following Section II reviews transnational IPR enforcement measures, and Section III briefly addresses global and local licensing practices. Based on this overview, the concluding section identifies three layers of IP governance on the Internet.

II. IPR Enforcement

3 Transnational IPR enforcement on the Internet occurs in two forms. One aspect concerns formal court decisions (sub-heading 1), the other self-regulatory measures implemented by intermediaries (sub-heading 2).

---

[6] Annette Kur in European Max Planck Group on Conflict of Laws in Intellectual Property (CLIP), *Conflict of Laws in Intellectual Property, The CLIP Principles and Commentary* (2013) paras 3:603.C01-3:604.C22.

[7] Cf Philip Jessup, *Transnational Law* (1956) 2; Thomas Schultz, 'Private Legal Systems: What Cyberspace Might Teach Legal Theorists' (2007) 10 Yale J L & Tech 151.

[8] To my knowledge, the only publication that explicitly addresses this issue, albeit not in systematic form, is Thomas Hoeren and Guido Westkamp, *Study on voluntary collaboration practices in addressing online infringements of trade mark rights, design rights, copyright and rights related to copyright* (2016) 36. See also Kristofer Erickson and Martin Kretschmer, 'Empirical Approaches to Intermediary Liability' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (2020) 105.

[9] Cf Art 11 TRIPS.

1. Takedown Orders of Courts: de iure and de facto Effects

4 According to the territoriality principle, court ordered injunctions and other remedies only concern activities in the territory of the IP law(s) pleaded and applied.[10] In practice, however, a court order to cease and desist making a certain content available on the Internet has, even if only one national IPR/law was considered, automatic extraterritorial effects because Internet users in other countries also lose the possibility to access the respective source, irrespective of whether or not the content infringed IPRs under the laws of these third countries.[11]

5 If the defendant can show that the upload in question is legal under certain IP laws, the proper reaction of a court in line with the territoriality principle is to explicitly limit the injunction to the countries whose IP laws were pleaded and violated against, and to order the defendant to geo-block access to the content at stake from these infringement territories only.[12] For example, a German court ordered a U.S. operator of a website which provides access to works in the public domain under U.S. law to prevent German users from accessing the writings of Thomas Mann and others whose works are still protected by copyright under German law within Germany.[13] The conflict between independently owned, equally legitimate trademark rights in identical or similar signs (e.g. *Merck Germany v. Merck U.S.*) is also resolved by obliging both parties to implement geo-targeting and geo-blocking measures so as to avoid consumer confusion in the markets in which each trademark owner enjoys exclusivity.[14] A counterexample proving the territoriality rule is the infamous Canadian-U.S.

---

[10] Graeme Dinwoodie in European Max Planck Group on Conflict of Laws in Intellectual Property (CLIP), *Conflict of Laws in Intellectual Property, The CLIP Principles and Commentary* (2013) paras 2:604.C01-N04.

[11] Marketa Trimble, 'The Territorial Discrepancy Between Intellectual Property Rights Infringement Claims and Remedies' (2019) 23 Lewis & Clark L Rev 501, 503–04.

[12] Geo-blocking has generally been accepted to accommodate global online communication with local laws. See *Yahoo! Inc v La Ligue Contre Le Racisme Et L'Antisemitisme* [2006] 433 F3d 1199, 1216-7 (public law); Opinion of Advocate General Szpunar, CJEU Case C-18/18 *Eva Glawischnig-Piesczek* ECLI:EU:C:2019:458, paras 100-1 (defamation); CJEU Case C-507/17 *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* ECLI:EU:C:2019:772, para 70 (data protection).

[13] Higher Regional Court Frankfurt am Main, 30.04.2019 - 11 U 27/18 - BeckRS 2019, 11210 – *Project Gutenberg*.

[14] See CJEU Case C-231/16 *Merck v Merck* ECLI:EU:C:2017:771; Alexander Peukert, 'The Coexistence of Trade Mark Laws and Rights on the Internet, and the Impact of Geolocation Technologies' (2016) 47(1)

jurisdictional conflict in *Google v. Equustek*. In this case, the Canadian Supreme Court explicitly ordered Google, on the basis and in furtherance of Canadian trade secrets law, to de-index certain websites not only from Google.ca but from any of its search results worldwide.[15] In a countermove, Google obtained a decision from a U.S. District Court declaring the Canadian global order to be unenforceable in the U.S. in view of the immunity of search engine operators under U.S. law.[16] At the same time, Google reterritorialized its search engine. Instead of allowing Internet users to circumvent the removal of search results by simply switching to another Google top level domain (TLD) – a possibility that concerned the Canadian Supreme Court and triggered its global response – Google now employs geolocation technologies that make certain that users see a version of the search results that is in accordance with the laws of the place from where the search is presumably conducted.[17] The Canadian global court order thus ultimately reinforced territorial fragmentation.

6 In most cases, however, the territorial overreach of takedown orders goes unnoticed. One reason for this is the quite advanced level of international harmonization in the area of IP. Cases where local IP laws diverge in meaningful ways are relatively rare. That, for example, current movies must not be made available on the Internet without prior authorization of the right holder is, by and large, a universally valid legal statement. In such clear cases, the practice of unrestricted takedown orders with de facto worldwide effects also appears legitimate. In hard cases of conflicts of IP laws or rights, however, cyberspace is split up via geo-blocking along the real-world borders between IP jurisdictions.

International Review of Intellectual Property and Competition Law 60-87.

[15] *Google Inc v Equustek Solutions Inc* (n 2) ("Google's argument that a global injunction violates international comity … is theoretical.").

[16] *Google v Equustek Solutions* [2017] WL 500834 (ND Cal). But see *Equustek Solutions Inc v Jack* [2018] British Columbia Supreme Court, [2018] 10 WWR 715 (Can) (dismissing an application to set aside or vary the global injunction). See also Robert Diab, 'Search Engines and Global Takedown Orders: Google v Equustek and the Future of Free Speech Online' (2019) <https://ssrn.com/abstract=3393171> accessed 15 September 2020; Michael Geist, 'The Equustek Effect: A Canadian Perspective on Global Takedown Orders in the Age of the Internet.' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (2020) 709.

[17] *Equustek Solutions Inc v Jack* (n 16); *Google LLC v CNIL* (n 12) at para 42.

2. Intermediaries' Enforcement Measures

7 The second, and practically much more important mode of transnational IPR enforcement on the Internet, concerns private self-regulation by intermediaries.

a) The Central Role of Intermediaries

8 Intermediaries providing services for online communication have for a long time occupied a central role in Internet governance in general and online IPR enforcement in particular. Firstly, "[n]othing happens online that does not involve one or more intermediaries" such as domain name registrars, access and host providers, search engines, advertising, and payment services.[18] Secondly, and in contrast to anonymous pirates of cyberspace, intermediaries are actual targets of enforcement efforts who conduct a lawful business as part of the formal economy.[19] Thirdly, they offer a solution for the problem of the scale of copyright and other IPR infringements online, which are so numerous that they could never be adjudicated in state court proceedings.[20] Through the code with which intermediaries operate their services, they are able to enforce IPRs in many cases – in the case of Google search, billions – at relatively little cost. The answer to the problem of IPR infringements via digital network technologies is indeed "in the machine", and these machines are controlled by private intermediaries.[21]

9 Until very recently, however, online intermediaries have not been considered direct infringers.[22] It is not the intermediaries that make copyrighted works available to the

---

[18] Jacqueline D Lipton, 'Law of the Intermediated Information Exchange' (2012) 64 Fla L Rev 1337; Derek E Bambauer, 'Middlemen' (2012) 64 Fla L Rev F 64; Graeme Dinwoodie, 'Who Are Internet Intermediaries?' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (2020) 37.
[19] On the difficulties to pursue individual IPR infringers see Yochai Benkler, *The Wealth of Networks* (2006) 396; Anupam Chander, *The Electronic Silk Road* (2013) 87-112 ("pirates of cyberspace").
[20] On the scale of cases as a characteristic feature of cyberlaw see David G Post, *In Search of Jefferson's Moose* (2009) 60-89.
[21] Charles Clark, 'The Answer to the Machine is in the Machine', in Bernt Hugenholtz (ed), *The Future of Copyright in a Digital Environment* (1999) 139; Maayan Perel and Niva Elkin-Koren, 'Accountability in Algorithmic Copyright Enforcement' (2016) 19 Stan Tech L Rev 473; Clement Salung Petersen and Thomas Riis, 'Private enforcement of IP law by internet service providers: notice and action procedures' in Thomas Riis (ed), *User Generated Law* (2016) 228, 239-40.
[22] Art 17 of the Council Directive 2019/790/EU of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ L130/92 (DSM Directive) (online content-sharing service providers perform an act of communication/making available to the public when they give the public access to copyright-protected content uploaded by their users).

public, sell counterfeit products and otherwise infringe IPRs, but their customers/users. Intermediaries are therefore liable for third-party infringements if at all only indirectly under additional requirements and to a limited extent. Standards vary according to the intermediary concerned and across IP jurisdictions,[23] but the basic dilemma and also the regulatory approach to intermediary liability is the same across the board. On the one hand, intermediaries' services are used in the course of IPR infringements, they are aware of illegal activity at least upon being notified accordingly, and they are in a position to do something about it. Thus, right holders and governments constantly pressure intermediaries to curb at least clear cases of piracy and counterfeiting. On the other hand, intermediaries provide per se neutral services that are widely used for perfectly legal and socially beneficial purposes. Consequently, intermediaries have been shielded from levels of liability that would amount to a general obligation to monitor their services or otherwise render their legitimate business model impossible.[24] For example, host providers and search engines have to expeditiously remove or disable access to IP-infringing content after a respective notification (notice and takedown, NTD). At the same time, they are neither liable vis-à-vis IPR holders until being notified of an infringement nor vis-à-vis their customers/users for good faith false positive takedowns.[25]

10 This framework opens up an "autonomy space", within which intermediaries are able to develop tailor-made IP policies for their services.[26] Such in-house solutions will generally be preferred to potentially disruptive, exogenous rules imposed by courts or

---

[23] Matthias Leistner, 'Intermediary Liability in a Global World' (March 2, 2019) in Tatiana Eleni Synodinou (ed), *Pluralism or Universalism in International Copyright Law* (Forthcoming) available at <https://ssrn.com/abstract=3345570> accessed 16 September 2020.

[24] Cf Lilian Edwards, *WIPO Report: Role and responsibility of internet intermediaries in the field of copyright and related rights* (WIPO 2005), <http://www.wipo.int/export/sites/www/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf> accessed 16 September 2020, 7-8; Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (2020).

[25] See 17 USC § 512(c), (g); Arts 14, 15 Council Directive 2000/31 of 8 June 2000 on electronic commerce [2000] OJ L 178/1 (E-Commerce Directive) and CJEU Case C-324/09 *L'Oréal SA and Others* ECLI:EU:C:2011:474, paras 106-44; Arts 18.81-2 Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP).

[26] Petersen and Riis (n 21) 228 et seq; Michael Andreas Kümmel, *Die Implementierung der Haftung von Host-Providern für Immaterialgüterrechtsverletzung* (2017) (documenting notice and takedown regimes of eBay, Amazon, Facebook, and YouTube).

legislators.[27] In developing their IP policies, intermediaries are not primarily guided by public policy goals but, as private corporations, by the aim to maximize profits. In the IP liability context, this means to navigate cost-efficiently between the Scylla of IP liability and the Charybdis of customers who are unsatisfied with an overly restrictive service. Regarding the territorial scope of IP policies, economies of scale militate in favor of service-wide, transnational standards instead of country-specific measures, implemented via costly geolocation technologies.[28] All these aspects support the emergence of private, transnational IP policies.

11 Yet, as the following examples demonstrate, the state has not left the stage.[29] Already by defining the standard of statutory IP liability, legislators and courts influence the content and territorial scope of intermediaries' IP policies. In addition, the European Commission and other governments have for a long time beset intermediaries to accept ever more concrete IP codes of conduct.[30]

---

[27] Matthew Sag, 'Internet Safe Harbors and the Transformation of Copyright Law' (2017) 93 Notre Dame L Rev 499, 542.

[28] Joel R Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1998) 76 Tex L Rev 553, 577–79 ("Technologically implemented rules apply throughout the relevant network. As such, Lex Informatica reaches across borders and does not face the same jurisdictional, choice of law problem that legal regimes encounter when networks cross territorial or state jurisdictional lines."); P Bernt Hugenholtz, 'Codes of Conduct and Copyright Enforcement in Cyberspace' in Irini A Stamatoudi (ed), *Copyright Enforcement and the Internet* (2010) 303-4.

[29] European Commission, 'Report on the functioning of the Memorandum of Understanding on online advertising and intellectual property rights' SWD(2020) 167 final/2, 4 (European Commission facilitates cooperation between IPR holders and online marketplaces); Michael D Birnhack and Niva Elkin-Koren, 'The Invisible Handshake: The Reemergence of the State in the Digital Environment' (2003) 8 Va JL & Tech 1–2; Uta Kohl, *Jurisdiction and the Internet* (2007) 265-70; Yochai Benkler, 'A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate' (2011) 46 Harv CR-CL Rev 311 ("regulation by raised eyebrow"); Hannah Bloch-Wehba, 'Global Platform Governance: Private Power in the Shadow of the State' (2019) 72 SMU L Rev 27.

[30] Cf Art 16 E-Commerce Directive (n 25) (codes of conduct); Art 17(10) DSM Directive (n 22) (best practices for cooperation between online content-sharing service providers and rightholders); Art 18.82(1)(a) CPTPP (n 25) (contracting parties shall incentivize cooperation between ISPs and copyright owners); Hugenholtz (n 28) 306; Natasha Tusikov, *Chokepoints: Global Private Regulation on the Internet* (2017); Martin Husovec, *Injunctions against intermediaries* (2017) 229 et seq; Salung Petersen and Riis (n 21) 230; Giancarlo Frosio, Algorithmic Enforcement Online' in Paul Torremans (ed), *Intellectual Property and Human Rights* (2020) 709.

b) Intermediaries' Enforcement Measures and Their Transnational Effect

12 Intermediaries' enforcement measures and their transnational effect vary according to the type of service concerned and the geographical scope of application of self-regulatory rules.

aa) Domain Name Registrars

13 In the case of domain name registrars, the combined efforts of trademark owners and governments led to a very early and well-known global regime, namely the "Uniform Domain Name Dispute Resolution Policy" (UDRP), adopted by the Internet Corporation for Assigned Names and Numbers (ICANN) in 1999, which is still in force today in its original version.[31] The emergence of the UDRP is tightly bound to U.S. law and policy.[32] After it had become settled case law that registering a trademark as a domain name in order to sell it to the corresponding trademark holder constitutes trademark infringement,[33] the U.S. legislature in 1999 extended trademark protection to address the problem of non-U.S. "cybersquatters". The Anticybersquatting Consumer Protection Act (ACPA) allows for *in rem* civil actions against domain name registrars based in the U.S. for the forfeiture or cancellation of a domain name or the transfer of a domain name from a foreign domain name holder to the owner of the respective mark. Notably, the statute grants immunity to domain name registrars unless they act in bad faith or recklessly disregard their duties under the statute.[34]

---

[31] See ICANN, Uniform Domain-Name Dispute-Resolution Policy (UDPR) <https://www.icann.org/resources/pages/help/dndr/udrp-en> accessed 16 September 2020 and, eg, Laurence R Helfer and Graeme B Dinwoodie, 'Designing Non-National Systems: The Case of the Uniform Domain Name Dispute Resolution Policy' (2001) 43 Wm & Mary L Rev 141; Jens Schovsbo, 'The private legal governance of domain names' in Thomas Riis (ed), *User Generated Law* (2016) 206. On the cheaper and faster "Uniform Rapid Suspension System" in the context of new gTLDs such as .bike, see ICANN, Uniform Rapid Suspension (URS) <https://www.icann.org/resources/pages/urs-2014-01-09-en> accessed 16 September 2020; James L Bikoff and others, 'The Uniform Rapid Suspension System: A New Weapon in the War against Cybersquatters' (2014) 6(3) Landslide 32.

[32] Marketa Trimble, 'Territorialization of the Internet Domain Name System' (2018) 45 Pepp L Rev 623, 661–62.

[33] *Panavision Int'l v Toeppen* [1998] 141 F3d 1316 (holding that pattern of offering domain names for sale to mark holders was "use in commerce" of the mark sufficient to violate Lanham Act).

[34] 15 USC § 1125.

14 Simultaneously, the privatization of the Internet was in full swing. In 1998, the U.S. Department of Commerce announced that the global Domain Name System was to be centrally controlled and coordinated by ICANN, a nonprofit California corporation, but that there should be competition between domain name registrars accredited by ICANN.[35] That, in turn, created the risk that non-U.S. cybersquatters could register trademark-protected signs with non-U.S. registrars beyond the reach of U.S. trademark law and the ACPA. In addition, the global Domain Name System highlighted the problem of conflicting trademark rights on the Internet. If the very same sign or confusingly similar signs can be trademark-protected in country A for company A, and in country B for company B, who is entitled to use the sign on the Internet?[36]

15 To address the looming enforcement and coordination problems, the U.S. government called upon the World Intellectual Property Organization (WIPO) to consult both trademark holders and members of the Internet community with the aim to develop recommendations for "a uniform approach to resolving trademark/domain name disputes involving cyberpiracy (as opposed to conflicts between trademark holders with legitimate competing rights)."[37] In accordance with this suggestion, the focus of the UDRP is on bad faith "cybersquatters". In a nutshell, the UDRP requires registrants and domain name applicants to submit to mandatory administrative proceedings in the event that a trademark holder asserts that (1) a registered domain name is identical or confusingly similar to a trademark, (2) the domain name holder has no rights or legitimate interests in respect of the domain name, and (3) the domain name has been registered and is being used in bad faith. If these requirements are met, a UDRP panel can order either the cancellation of the domain name or its transfer to the complainant, which is to be carried out by the registrant concerned after ten business days.[38] Through its inclusion in registration agreements of all ICANN-accredited registrars, the UDRP has become a global legal standard, binding upon all holders of generic and

---

[35] On the formation of ICANN see A Michael Froomkin, 'Wrong Turn in Cyberspace: Using Icann to Route Around the Apa and the Constitution' (2000) 50 Duke LJ 17, 50–51; US Department of Commerce, 'Management of Internet Names and Addresses' (1998) 63 FED REG 31,741 <https://www.govinfo.gov/content/pkg/FR-1998-06-10/pdf/98-15392.pdf> accessed 16 September 2020.
[36] See *Merck v Merck* (n 14).
[37] US Department of Commerce (n 35).

numerous country-code TLDs, irrespective of the domicile of the registrant and the other parties involved. The vast majority of many thousand UDRP panel decisions has been in favor of trademark owners and has not given rise to an admissible review by state courts.[39]

16 From the perspective of traditional trademark law and its territorial fragmentation, the long-term success of the UDRP should still come as a surprise. The complainant only needs to show ownership of one single national trademark to be possibly allocated a generic TLD such as .com, which is useful for worldwide commercial activities.[40] Thus, the UDRP equips national trademarks with worldwide effects. This globalization of national trademarks is, however, acceptable because the UDRP only targets a limited set of simplistic cases. Firstly, the UDRP is only concerned with domain names and not with the content accessible via that domain. Secondly, the person having registered the domain in question must not have any rights or legitimate interests in respect of the name. Disputes between holders of equally legitimate national rights in identical/similar domains are beyond the scope of the UDRP and remain subject to the territorially fragmented system of IP law.[41] And thirdly, the registration must have occurred in "bad faith", for example, for the purpose of selling the domain to the complainant or for misleadingly generating website traffic.[42] There apparently is a stable, rough global consensus[43] that such bad faith "cybersquatters" do not deserve forbearance. Any valid national trademark suffices to expel them from the global domain name system.

---

[38] UDRP (n 31) paras 3, 4.
[39] Laurence R Helfer, 'Whither the UDRP: Autonomous, Americanized, or Cosmopolitan? (2004) 12 Cardozo J Int'l & Comp L 493, 494–95 (barely 1% of all UDRP panel rulings have been submitted for review by national courts); Annemarie Bridy, 'Notice and Takedown in the Domain Name System: Icann's Ambivalent Drift into Online Content Regulation' (2017) 74 Wash & Lee L Rev 1345, 1357–58 (in WIPO proceedings, registrants have prevailed in only 12% of cases); WIPO Conference – As the UDRP Turns 20: Looking Back, Looking Ahead <https://www.wipo.int/portal/en/news/2019/article_0050.html> accessed 16 September 2020 (over 45.000 UDRP cases have been filed with WIPO's Arbitration and Mediation Center).
[40] Cf para 1.2.6.1 URS (n 31) (the complaint has to show that the complainant holds "a valid national or regional registration and that is in current use").
[41] Peukert (n 14) 60-87.
[42] UDRP (n 31) para 4(b).
[43] On the concept of "rough consensus and running code" see Post (n 20) 136-7; Gralf-Peter Callies and Peer Zumbansen, *Rough Consensus and Running Code* (2010) 135-6.

17 The fragility and limits of this "consensus" became apparent, however, when U.S. copyright holders tried to get ICANN and its accredited registrars involved in a copyright enforcement scheme, according to which domain names for notified "pirate sites" would have been cancelled. If this plan had materialized, private IPR enforcement via the domain name system would have reached, for the first time, beyond the domain name/trademark level deep into the content layer.[44] After a "trusted notifier" copyright enforcement program between the Motion Picture Association of America and two registry operators for new generic TLDs (one based in the U.S., the other in Abu Dhabi) had been publicly revealed, registrars, however, quickly backpedaled.[45] ICANN's current Registry Agreement with registrars of new generic TLDs requires registrars to prohibit new generic TLD holders from engaging in "piracy, trademark or copyright infringement … counterfeiting or otherwise engaging in activity contrary to applicable law", and to provide "(consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name".[46] There is, however, no out-of-court online dispute resolution system comparable to the UDRP in place to enforce these directives.

bb) Access Providers

18 To engage domain name registrars in the enforcement of copyright and other content-related laws would indeed be problematic because of the sweeping effects of a domain name cancellation, which de facto disconnects the server hosting the (allegedly) infringing websites from the Internet. By comparison, less effective and less far-reaching blocking orders against access providers, which can also be implemented via the

---

[44] Bridy (n 39) 1345, 1346–49, 1359–62. The seizure/disconnection of domains by public authorities in the context of criminal proceedings remains unaffected; see Jack Mellyn, '"Reach Out and Touch Someone": The Growing Use of Domain Name Seizure As A Vehicle for the Extraterritorial Enforcement of U.S. Law' (2011) 42 Geo J Int'l L 1241, 1242–43; IACC (2017) <https://www.iacc.org/media/the-international-anticounterfeiting-coalition-and-city-of-london-police-partner-to-protect-consumer> accessed 16 September 2020 (announcing cooperation between the International AntiCounterfeiting Coalition (IACC) and the City of London Police Intellectual Property Crime Unit (PIPCU) to take down websites selling counterfeits through the IACC RogueBlock Program).

[45] See Annemarie Bridy, 'Addressing Infringement: Developments in Content Regulation in the US and the DNS' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (2020) 632, 637-45.

[46] Specification 11, section 3(a) Base New gTLD Registry Agreement (31 September 2017) <https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html>

domain name system,[47] are considered by the European Court of Human Rights as an "extreme measure" that "deliberately disregards the distinction between the legal and illegal information the website may contain, and renders inaccessible large amounts of content which has not been identified as illegal".[48]

19 Because of these concerns and the neutral, "mere conduit" role of access providers regarding the content their services transmit, these ISPs enjoy broad immunities and had for quite a while managed to avoid getting involved in IPR enforcement online.[49] That outsider position came under fire, however, with the advent of massive unauthorized peer-to-peer file sharing in the early 2000s, which copyright holders could not effectively curb by going after anonymous individual infringers.[50] In addition, in the fight against counterfeit goods sold on the Internet, right holders increasingly spotlighted access providers as possible targets.[51]

20 An initial type of private enforcement schemes involving access providers were so-called "graduated response" procedures, which access providers from several countries adopted "voluntarily" after intense pressure by right holders and governments.[52] The concept of these programs was that copyright owners would report dynamic IP addresses used for illegal file sharing to access providers. The access provider whose subscriber had used the IP address at the relevant time then sent a warning to that user. After three to six warnings ("strikes"), access providers were to sanction their subscribers by throttling bandwidth or even by temporarily cutting off repeat infringers from the Internet.

---

accessed 22 September 2020.

[47] *Cartier International AG v British Sky Broadcasting Ltd* [2014] EWHC 3354 (Ch), [2015] RCP 7, para 25.

[48] ECtHR Case 12468/15 *Flavus v Russia* para 37.

[49] Cf 17 USC § 512(a); Art 12 E-Commerce Directive (n 25).

[50] Cf Alexander Peukert, 'Why do "good people" disregard copyright on the internet?' in Christophe Geiger (ed), *Criminal Enforcement of Intellectual Property: A Handbook of Contemporary Research* (2012) 151.

[51] This is true in particular for the UK. See *Cartier International AG v British Telecommunications Plc* [2018] UKSC 28; *Nintendo Co Ltd v Sky UK Ltd* [2019] EWHC 2376 (Ch).

[52] Annemarie Bridy, 'Graduated Response American Style: "Six Strikes" Measured Against Five Norms' (2012) 23 Fordham Intell Prop Media & Ent LJ 1, 3–6; Rebecca Giblin, 'Evaluating Graduated Response' (2014) 37 Columbia Journal of Law & the Arts 147.

21 These measures were not well received by the general public and have largely been abandoned.[53] Instead of going after individual Internet users, a second type of IPR enforcement measure involving access providers gained prominence: website blocking. In 2014, the CJEU held that EU Member States have to ensure that copyright holders can apply for an injunction against access providers to prohibit them from allowing their customers access to a copyright infringing website if such an order does not unnecessarily deprive Internet users of access to lawful information.[54] This ruling supports collaboration between right holders and access providers to make sure that all ISPs block certain websites, and that if the infringing content is moved to another domain, this new page will also be blocked.[55]

22 If implemented in these ways, website blocking can be an effective IPR enforcement measure.[56] Its geographical reach is, however, rather limited and rarely ever transnational. The reason is that, in contrast to domain cancellations by registrars, website blocking by access providers does not apply to the single source of the infringement but attaches to the recipients who try to access the source. In addition, only the customers of a particular access provider are affected by blocking measures. And since providing access to the Internet requires some control over physical infrastructure, access providers do business and have customers within clearly defined areas, typically within a nation state. Website blocking thus occurs country-by-country, based on the local IPR regime vis-à-vis local access providers and their customers.[57] In this case, the territoriality of IPRs conforms to the fragmentation of telecommunications markets.

---

[53] See Christophe Geiger 'Honourable Attempt but (ultimately) Disproportionately Offensive against Peer-to-Peer on the Internet (HADOPI) – A Critical Analysis of the Recent Anti-File-Sharing Legislation in France' (2011) 44 Intl Rev of Intell Prop and Comp L 457.
[54] CJEU Case C-314/12 *UPC Telekabel Wien v Constantin Film Verleih* ECLI:EU:C:2014:192, paras 32, 64.
[55] See Hoeren and Westkamp (n 8) 269 et seq (Danish code of conduct).
[56] Ibid 269 et seq (20% drop in P2P file sharing in Denmark).
[57] See eg Dirk Visser, 'Conclusions Sought: Blocking Orders – A View from the EU' in Ysolde Gendreau (ed), *Copyright in Action* (2019) 326-9 (describing how rightholders achieved that the "Pirate Bay" website was blocked by all Dutch access providers).

cc) Host Providers and Search Engines

23 The two intermediaries examined above occupy very different roles in cyberspace. Whereas ICANN and its accredited registrars control the basic domain name system, access providers operate at the ends of the Internet. The geographical scope of the measures taken by these intermediaries differs accordingly. Domain name cancellations are effective across the entire Internet and thus globally, website blocking by an access provider only affects its customers, i.e. residents of a certain state.

24 Host providers and search engine operators control still other infrastructures. The former are able to directly interfere with IPR infringing communication by preventing uploads *ex ante*, by taking them down and by making sure they stay down.[58] Search engines, in contrast, can only reduce the findability of an illegal source by removing search results; the infringing websites themselves remain accessible.[59] The power of host providers and search engines to regulate online communication across borders and potentially even worldwide is nevertheless similar. Both are, roughly speaking, situated somewhere between domain name registrars and access providers. Their intermediary services are less basic than those of ICANN but more central than the peripheral operations of access providers.

25 Correspondingly, IP policies of host providers and search engines may, but need not necessarily, have transnational or even global implications.[60] The territorial effect of their IP enforcement measures depends upon technical, legal and economic circumstances. If applicable laws do not define the required or permissible geographical scope of removals or that question is unsettled,[61] host providers and search engines are

---

[58] Cf 17 USC § 512(c); *L'Oréal v eBay International* (n 25) paras 125-44; Art 17(4) DSM Directive (n 22).
[59] 17 USC § 512(d); CJEU Case C-131/12, *Google Spain v AEPD* ECLI:EU:C:2014:317, paras 80-8; *Google Inc v Equustek Solutions Inc* (n 2).
[60] Cf Opinion of Advocate General Szpunar, CJEU Case C-18/18 *Glawischnig-Piesczek v Facebook Ireland* ECLI:EU:C:2019:458, para 77 (Facebook Ireland does not deny that it is in a position to ensure such removal worldwide).
[61] As in the case of EU law regarding the indirect liability of search engines for personality rights and data protection violations; cf *Glawischnig-Piesczek* (n 60) paras 48-53 (EU law does not preclude a court of a Member State "from ordering a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law"); *Google LLC v Commission nationale de l'informatique et des libertés* (n 12), para 72 ("EU law does not currently

left with an individual, "autonomous" decision whether to adopt and implement one single IP policy across the service or whether to reproduce the territorial fragmentation of IP and other laws by splitting up their service into country-specific versions with separate IP takedown/delisting policies. At the end of the day, this is a private business decision that can change over time and that is typically not publicly announced.[62] One already mentioned example concerns Google's search engine, which was, presumably also in light of court proceedings pending in various jurisdictions, restructured to the effect that it is not the user, by entering a particular top level domain such as .ca or .de, who determines the search result version displayed, but Google itself via geolocation technologies.[63] Host providers also sometimes use different domains for different countries, whereas others operate with a universal .com domain.[64]

26 In spite of the notorious lack of transparency in this realm, there are several reasons to assume that most IPR removals by host providers and search engine operators have service-wide and thus transnational effects. This is necessarily the case if a service that hosts a website takes that website down. Unless another host provider steps in, the content will become inaccessible for all Internet users worldwide. For example, a Dutch NTD code of conduct required the takedown of websites hosted in the Netherlands by Dutch providers if these were "evidently illegal" under Dutch copyright law.[65] Every element of this private ordering scheme is tied to the Netherlands – except for the effects of website takedowns, which are global.

27 Removals from market-dominant online platforms and search engines also significantly reduce illegal online communication. A service-wide measure of a big tech company might not be literally global (because the service may not be available in all countries, most notably China), but content delisted from, e.g. Google search effectively

---

require that the de-referencing granted concern all versions of the search engine in question, it also does not prohibit such a practice").

[62] Critical eg P Bernt Hugenholtz, 'Codes of Conduct and Copyright Enforcement in Cyberspace' in Irini A Stamatoudi (ed), *Copyright Enforcement and the Internet* (2010) 307.

[63] Supra n 17.

[64] European Commission, 'Report on the functioning of the Memorandum of Understanding on the sale of counterfeit goods on the internet' SWD(2020) 166 final/2, 8.

[65] Hoeren and Westkamp (n 8) 213.

disappears from the eye of the public in many countries.[66] Considerations of cost-efficiency will generally prompt online platform and search engine operators to implement IP removals across their services and thus also across IP jurisdictions. Accordingly, U.S. big tech companies have globalized their homegrown NTD procedures for all countries in which they operate.[67] In its "transparency report", Google states that its web form for copyright infringement notices "is consistent with the [U.S.] Digital Millennium Copyright Act (DMCA) and provides a simple and efficient mechanism for copyright owners *from countries/regions around the world*."[68] Facebook has likewise stated its intention to combat copyright and trademark infringement with a "*global* notice-and-takedown program".[69]

28 Although these statements only concern the uniformity of IP procedures, there is no reason to believe that takedowns resulting therefrom are implemented in a fragmented, country-specific way, e.g. only for the country from where the infringement notice was submitted. If there is only one IP policy, it will presumably be executed uniformly across the platform. Moreover, IP infringements are often also considered violations of the platforms' terms of service, which are, in the case of YouTube, "enforced consistently across the globe, regardless of where the content is uploaded. When content is removed for violating our guidelines, it is removed globally."[70] Repeat infringer policies, as implemented by most online marketplaces and user generated content (UGC) platforms,[71] necessarily produce this service-wide effect. If a subscriber's account is temporarily suspended or altogether terminated, that person simply cannot use the platform to make IPR infringing content available anywhere.

---

[66] *Google Spain v AEPD* (n 59) para 80.

[67] Petersen and Riis (n 21) 235-6; Kümmel (n 26) 33-36 (concerning Facebook's copyright policies); Sharon Bar-Ziv and Niva Elkin-Koren, 'Behind the Scenes of Online Copyright Enforcement: Empirical Evidence on Notice & Takedown' (2018) 50 Conn L Rev 339, 352–53 (de facto global standard).

[68] Google Transparency Report, 'Content delistings due to copyright' <https://transparencyreport.google.com/copyright/overview?hl=en> accessed 23 September 2020 (emphasis added).

[69] Facebook Transparency, 'Intellectual Property' <https://transparency.facebook.com/intellectual-property> accessed 23 September 2020 (emphasis added).

[70] Google Transparency Report, 'YouToube Community Guidelines enforcement' <https://transparencyreport.google.com/youtube-policy/removals?hl=en> accessed 23 September 2020.

[71] Cf European Commission (n 64) 16; IACC MarketSafe <https://www.iacc.org/online-initiatives/marketsafe> accessed 23 September 2020 (collaboration between trademark owners and

29 Although its geographical scope is not explicitly stated, the EU Memorandum of Understanding (MoU) "on the sale of counterfeit goods via the internet", agreed upon in 2011 between all major online marketplaces and numerous IPR holders, confirms that service-wide approach to IPR enforcement.[72] On the one hand, the MoU defines "counterfeit goods" as "non-original physical goods manufactured without the consent of the Rights Owner which infringe [a registered trade mark, design right or copyright], pursuant to applicable Member State or EU law".[73] The European Commission also stresses that signatories of the MoU must comply with EU and national laws and reports that online platforms are concerned about the sometimes unclear geographical scope of the IPRs submitted as being infringed.[74] On the other hand, platform providers commit to implement NTD procedures so that notified offers become "unavailable to the general public through the Internet Platform", i.e. service-wide.[75] Preventive measures, the precise layout of which remains at the discretion of platform providers, also have to prevent counterfeit goods from being offered or sold "through their services".[76] The European Commission furthermore reports that the signatories of the MoU have set up dedicated internal teams responsible for IPR enforcement "globally".[77] It finally hopes to have facilitated a "standard" also for the "international level".[78]

30 Again as a kind of counterexample proving the rule of transnational enforcement, ISPs strongly oppose service-wide ("global") IP policies when it comes to measures beyond simple NTD procedures and discretionary preventive measures,[79] or when these programs are to be extended beyond clear copyright, trademark and design rights

---

Alibaba led to the permanent removal of 15.000 sellers from Alibaba's platforms).

[72] EU Memorandum of Understanding (MoU) on the sale of counterfeit goods on the internet, Ref Ares(2016)3934515-26/07/2016 <https://ec.europa.eu/growth/industry/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en> accessed 23 September 2020.

[73] MoU Counterfeit Goods (n 72) para 3.

[74] European Commission (n 64) 15, 25.

[75] MoU Counterfeit Goods (n 72) paras 5, 18.

[76] Ibid, para 27.

[77] European Commission (n 64) 16.

[78] Ibid 38.

[79] Cf MoU Counterfeit Goods (n 72) para 27 s 2 ("The measures taken by Internet Platforms shall be at their discretion").

infringements, i.e. beyond “piracy” and “counterfeiting”. If big tech accepts such additional obligations at all, it only does so on a country-by-country basis.

31 For example, in 2007 Google and Facebook rejected the adoption of “Principles for User Generated Content Services”, which included filtering obligations for the U.S. market.[80] A 2017 UK “Code of Practice on Search and Copyright” in which Google et al. voluntarily agreed to, *inter alia*, automatically demote “infringing websites” in the search results and prevent the generation of autocomplete suggestions leading consumers towards those sites, is explicitly limited to search results “returned to consumers in the UK”.[81] YouTube’s Content ID system, with which the company turned its copyright liability risk into a money making machine, also functions country-specific. Under this program, registered copyright owners can submit video files to YouTube which then scans all user uploads against its reference database.[82] When content in a video on YouTube matches a work in the reference database, right holders receive an alert and can decide whether they want the content to be blocked, monetized or whether they prefer to track the video’s viewership statistics. Any of these actions can be country-specific, i.e. “a video may be monetized in one country/region and blocked or tracked in another”.[83] Whereas YouTube advertises this private NTD+ system as a great success, it intensively lobbied against the EU’s move to make its adoption mandatory.[84] To give one final example, the transparency reports YouTube, Facebook and other large social media platforms are obliged to produce under a German Anti-Hate-Speech-Law demonstrate that this “Network Enforcement Act” is implemented only for users in Germany. If YouTube et al. are notified of an alleged violation of the German act, they

---

[80] See ‘The Principles for User Generated Content Services: A Middle-Ground Approach to Cyber-Governance’ (2008) 121 Harv L Rev 1387, 1400 (caveat for voluntary application of the principles “outside the United States”).

[81] See Code of Practice on Search and Copyright [2017] available at <https://www.eff.org/deeplinks/2017/03/foia-uncovers-part-uk-shadow-regulation-search-engines-and-copyright#footnoteref1_emf9g2x> accessed 23 September 2020.

[82] Taylor B Bartholomew, ‘The Death of Fair Use in Cyberspace: Youtube and the Problem with Content ID’ (2013) 13 Duke L & Tech Rev 66.

[83] YouTube Help, ‘How Content ID works’ <https://support.google.com/youtube/answer/2797370?hl=en> accessed 23 September 2020; Christina Angelopoulos and others, *Study of fundamental rights limitations for online enforcement through self-regulation* (2016) 65.

[84] See Art 17(4)(b) DSM Directive (n 22); YouTube Help, ‘Updates on Article 17 (formerly Article 13)’ <https://support.google.com/youtube/thread/17592587?hl=en> accessed 23 September 2020.

apply, in a first step, their global community standards. Only if a post is found to be in conformity with this universal standard, is it, in a second step, measured against the German statute. If a content passes community standards but fails German law, it is removed only for Germany but remains accessible in all other countries.[85]

dd) Follow the Money: Advertising and Payment Services

32 IP infringers acting for profit not only depend on the services of domain name registrars and various ISPs, but furthermore on advertising and payment services. If no ads appeared on illegal streaming sites and no payment transactions were executed for counterfeiters, these actors would quickly be forced out of their illegal business. Although it is highly questionable whether advertisers, providers of online ad services such as Google AdSense, and payment processors such as PayPal are indirectly liable for IP infringements committed by their customers/partners, these intermediaries have in the second decade of the 21st century become the target of an IP enforcement strategy called "follow the money".[86]

33 In several countries, right holder associations, advertisers (brand owners) and providers of online ad and consumer tracking services have agreed to procedures that aim at avoiding the placement of ads on websites "which have no substantial legitimate uses".[87] To this end, right holders, sometimes in collaboration with public authorities such as the London Police Intellectual Property Crime Unit, have compiled a database of IP infringing websites and share this with advertisers, who in turn instruct online intermediaries (e.g. Google) to prevent the appearance of their ads on these blacklisted

[85] Lena Isabell Löber and Alexander Roßnagel, 'Das Netzwerkdurchsetzungsgesetz in der Umsetzung' (2019) Multimedia und Recht 71-2.
[86] EU: European Commission, 'Towards a modern, more European copyright framework' COM(2015) 626 final/11; European Commission (n 29) 3. US: Annemarie Bridy, 'Internet Payment Blockades' (2015) 67 Fla L Rev 1523, 1529–30; Erika Douglas, 'Paypal Is New Money: Extending Secondary Copyright Liability Safe Harbors to Online Payment Processors' (2017) 24 Mich Telecomm & Tech L Rev 45.
[87] Section I 1, EU Memorandum of Understanding (MoU) on online advertising and IPR (2018) <https://ec.europa.eu/growth/industry/intellectual-property/enforcement/memorandum-of-understanding-online-advertising-ipr_en> accessed 23 September 2020; WIPO Advisory Committee on Enforcement, 'The building respect for intellectual property database project' (2019) WIPO/ACE/14/9, 2 ("pirate websites").

outlets.[88] Despite the fact that ad intermediaries again operate at scale and therefore have an economic interest to apply such blacklisting practices across their services, the self-regulatory codes on point explicitly take a country-by-country approach. The memorandum facilitated by the European Commission is "limited for each signatory to services provided in the States that are Contracting Parties to the European Economic Area", an Austrian ethics code only covers pirate websites directed to an Austrian audience, UK Good Practice Principles on point apply to websites targeting UK users, and so on.[89] This restrictive attitude towards IP policies in the advertising context stands in stark contrast to service-wide and thus "global" NTD procedures. It may reflect the much weaker legal case for holding advertisers and ad intermediaries accountable for IP infringements on third-party websites. Whereas there is a rough global consensus that host providers and search engines have to remove apparent IP infringements, there is no such agreement regarding the ad industry.[90]

34 This weakness has been remedied, however, by a remarkable intervention by the World Intellectual Property Organization (WIPO). After having secured a mandate from its member states, WIPO developed, and in 2019 started, the "WIPO ALERT" online platform, which functions as a global hub for national IP ad programs.[91] Upon signing a letter of understanding with WIPO, "Authorized Contributors" from any of WIPO's 193 member states can upload lists of copyright infringing website URLs to WIPO's database. Advertisers, advertising agencies and their technical service providers from any other WIPO member state can apply to become "Authorized Users" of WIPO ALERT. Following a check on their "bona fides", they can access and automatically implement the blacklists collected "from around the world".[92] As with the European

---

[88] Hoeren and Westkamp (n 8) 103 et seq (Austrian "ethics code"), 147 et seq (UK "Good Practice Principles for the Trading of Digital Display and/or Audio Advertising"); WIPO Advisory Committee on Enforcement (n 87) 2. On the complex structure and functioning of the online ad industry cf Michail Batikas, Jörg Claussen and Christian Peukert, 'Follow the Money: Online Piracy and Self-Regulation in the Advertising Industry' (2019) 65 International Journal of Industrial Organization 121-151.

[89] EU MoU Advertising (n 87) 2; White Bullet Solutions, *Study on the impact of the Memorandum of Understanding on online advertising and intellectual property rights on the online advertising market* (2020) 9; Hoeren and Westkamp (n 8) 111, 180; WIPO Advisory Committee on Enforcement (n 87) 2.

[90] European Commission (n 29) 12 (signatories will look into how to duplicate and expand the MoU "if possible, outside the EU").

[91] WIPO Alert <https://www.wipo.int/wipo-alert/en/> accessed 23 September 2020.

[92] WIPO Advisory Committee on Enforcement (n 87) 3-4, 7 ("the operation is entirely seamless and

Commission and other public authorities, WIPO describes its role as that of a neutral facilitator of legitimate enforcement practices. WIPO also expressly points out that it does not assert "that any particular site has, as a matter of law, infringed copyright". Rather, the blacklisted "sites of concern" are defined as "an online location which is reasonably suspected by an Authorized Contributor of deliberately infringing or facilitating the infringement of copyright and related rights, *whether in its country of establishment or elsewhere*".[93] This definition is inspired by Sec. 115A of the Australian Copyright Act, which provides for blocking orders against access providers under the condition that "the primary purpose of the online location is to infringe … copyright (*whether or not in Australia*)".[94] WIPO accordingly maintains that in practice only "invariably flagrant facilitators of copyright infringement" are covered by the ALERT database and thus cut-off from the global flow of advertising revenues.[95]

35 The second target of "follow the money" approaches are providers of online payment services like PayPal and credit card companies like Visa or Mastercard. These intermediaries are powerful because they are able to monitor suspicious merchants and link their activity across different banks. Whereas Europe appears to be the hot spot of efforts to get the highly diversified and geographically dispersed advertising industry on board,[96] the U.S. government has encouraged and supported an initiative called "RogueBlock®", which was launched in 2012 and now includes many of the biggest payment providers in the world. RogueBlock® was brokered by the Washington, D.C.-based International AntiCounterfeiting Coalition (IACC), a non-profit organization devoted solely to combating product counterfeiting and piracy, whose membership comprises more than 250 companies and organizations from 40+ countries.[97] RogueBlock® offers IACC's members the possibility to report online sellers of counterfeit or pirated goods directly to credit card and financial service companies with the goal of

---

requires no human intervention").
[93] WIPO Advisory Committee on Enforcement (n 87) 3-4 (emphasis added).
[94] See sec 115A Copyright Act 1968, as of 1 January 2019 <https://www.legislation.gov.au/Details/C2019C00042> accessed 23 September 2020 (emphasis added) and WIPO (n 87) 4 with fn 5.
[95] See WIPO Advisory Committee on Enforcement (n 87) 7 (WIPO cooperating with the European Commission in this field).
[96] Ibid 3-4.

facilitating prompt action against those merchants. According to the IACC, the program has terminated over 5,000 merchant accounts and impacted over 200,000 websites.[98] The geographical scope of the scheme is global in the sense that it does not matter where the "rogue" websites are hosted or the "rogue" merchants domiciled.[99] Instead, RogueBlock® is triggered as soon as goods offered through a website do not comply with IP laws in either the country of origin or the country of destination. Any transaction that is not in full "dual jurisdictional compliance" at the places of origin and destination is considered illegal. Merchants engaging in such illegal activity risk being cut-off from the global payment system, even if their offerings are lawful at their domicile and/or in third countries.[100]

c) Summary

36 The review of intermediaries' IP enforcement measures and accompanying codes of conduct demonstrates that most of them are transnational in scope. From a legal perspective, this finding can be explained with the focus of all regimes on plain infringements (cybersquatters, piracy, counterfeiting, "rogue" merchants). Hard cases of conflicts of IP laws/rights are, instead, resolved in a country-specific way according to the territoriality principle. From a technological perspective, transnational measures typically attach to the source of the infringement (domain name cancellations, takedowns, termination of payment accounts). Measures that instead apply to the recipient's end of the communication, i.e. website and advertisement blocking, are generally local in effect, but WIPO's remarkable ALERT database aims to make advertisement blocking global, too. Ultimately, only website blocking by access providers remains tied to certain real-world territories. The reason is that access providers operate on the physical layer of the Internet, and this tangible infrastructure is located in a particular country.

---

[97] Website of IACC <https://www.iacc.org/> accessed 23 September 2020.
[98] IACC RogueBlock <https://www.iacc.org/online-initiatives/rogueblock> accessed 23 September 2020; Bridy (n 86); Aniket Kesari and others, 'Deterring Cybercrime: Focus on Intermediaries' (2017) 32 Berkeley Tech LJ 1093, 1128.
[99] Hoeren and Westkamp (n 8) 346.
[100] Critical of this extraterritorial effect Bridy (n 86) (calling for a "zoning" of online payment blockades to only apply to transactions involving U.S. customers).

III. Licensing IPRs

37 Instead of prohibiting the use of protected IP by enforcing their rights, right holders are alternatively free to grant licenses and thus authorize uses. Whereas the territoriality principle complicates transnational IP enforcement on the Internet, the existing legal framework is in fact conducive to global online licensing.

38 Firstly, the rules governing initial ownership of IPRs are by and large uniform around the world, ensuring that the same person, in particular the author of a work and the one who first files for a patent or other registered IPR, acquires the complete bundle of national IPRs. If the rules on initial ownership diverge (author versus employer/commissioner; first-to-file versus first-to-invent), the parties involved share an interest in avoiding a split of initial and subsequent chains of titles in the same IP. Accordingly, courts presume that all relevant rights have been implicitly transferred to one single entity.[101] That global right holder is, secondly, at liberty to exercise her "private"[102] territorial rights uniformly at a global scale, be it by producing and selling IP-protected products on the world market or by granting a worldwide license to one single licensee.

39 In practice, however, IPRs are often monetized on a country-by-country basis. A global "celestial jukebox" as imagined by Paul Goldstein in the early 1990s, where users could access any content from any place at any time in exchange for a (micro)payment has yet to materialize.[103] According to a 2017 report by the European Commission on e-commerce in the EU, this is also true for the online commercialization of copyright-protected content in the "Digital Single Market". According to the Commission, a "majority of online digital content seems to be made available to users prevalently on a national basis, or for a territory covering two to four Member States, in the latter case when they share a common language".[104] The Commission further reports that "70% of digital content provider respondents restrict access to their online digital content

---

[101] Cf German Federal Court of Justice, case X ZR 14/17, openJur 2019, 1813, paras 83-107 (concerning the transfer of a right of priority); Josef Drexl in European Max Planck Group on Conflict of Laws in Intellectual Property (CLIP), *Conflict of Laws in Intellectual Property, The CLIP Principles and Commentary* (2013) paras 3:201.C01-N24.
[102] See preamble, TRIPS.
[103] Paul Goldstein, *Copyright's Highway: From Gutenberg to the Celestial Jukebox* (2003) 132 et seq.

services from other Member States".[105] Geo-blocking is implemented with regard to all types of digital content except for news products, and it is most prevalent in agreements for films, sports and TV series.[106] What is true for the EU Single Market is all the more true for the global market. Not surprisingly therefore, YouTube's Content ID program allows right holders from all over the world to control their content on the platform in a country-specific way so that "a video may be monetized in one country/region and blocked or tracked in another".[107] Shira Perlmutter, currently the Chief Policy Officer and Director for International Affairs at the U.S. Patent and Trademark Office and formerly a high-ranking IP executive in the music and movie industries also believes that "territoriality will endure for the foreseeable future."[108]

40 Aside from the online music sector, where national collective management organizations are important players who bridle at giving up their national monopolies,[109] the global legal framework is, as explained, not the prime reason for the persistence of territorial licensing and geo-blocking. Instead, right holders split up geographical markets because they consider this the right business decision. Product and price differentiations indeed respond to divergent local demand and purchasing power and thus promise maximum profits.[110] Geo-blocking to this end is furthermore supported by laws that prohibit the circumvention of technological protection measures.[111]

41 Authorized global access is, conversely, never coupled with a direct payment requirement. Instead, the right holder provides access for anyone in any country for free

---

[104] European Commission, 'Final report on the E-commerce Sector Inquiry' SWD(2017) 154 final/255-6.
[105] Ibid.
[106] Ibid.
[107] Supra n 83.
[108] Shira Perlmutter, 'Making Copyright Work for A Global Market: Policy Revision on Both Sides of the Atlantic' (2014) 38 Colum JL & Arts 49, 67–68; Tarja Koskinen-Olsson, 'Multi-Territorial Licenses' in José Maria Torres Caicedo, *Dissemination and Management of Works of Authorship on the Internet* (2018) 377-385 (trend towards multiterritorial licensing).
[109] See Arts 23-32 Council Directive 2014/26/EU of 26 February 2014 on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market [2014] OJ L 84/72 (setting out rules in support of multi-territorial licenses for online rights in musical works).
[110] William W Fisher III, 'Property and Contract on the Internet', (1998) 73 Chicago-Kent L Rev 1203.
[111] Arts. 11, 12 World Copyright Treaty (adopted 20 December 1996, entered into force 6 March 2002) 2186 UNTS 121 (WCT); Arts. 18, 19 WIPO Performances and Phonograms Treaty (adopted 20 December 1996, entered into force 20 May 2002) 2186 UNTS 203 (WPPT); Tatiana Eleni Synodinou,

and may, as the case may be, try to monetize her Open Content indirectly, in particular via advertising. Content categories that are particularly often distributed in this way include news, academic writings, software, and various types of non-professional UGC. Numerous licensing standards are available for this mode of distribution, notably various Free and Open Source Software and Creative Commons licenses.[112] Where no such formal license is adopted, courts interpret the free availability of copyright-protected content as an implied authorization by the right holder of foreseeable, commonly accepted Internet re-uses such as the copying and making available of pictures by search engines.[113] Both formal and implied Open Content licenses authorize uses in all countries, i.e. globally.

42 In sum, authorizations to use protected IP across the entire Internet are less prevalent than one might expect. Markets for fee-based services remain territorially fragmented. Global lawful access is practically limited to Open Content, which typically does not include the most popular and in that sense valuable works.[114]

IV. Conclusion

43 This article has brought together a dizzying array of IP governance practices on the Internet, whose varying geographical scopes are caused by a complex mixture of legal, technical and economic factors. It is, however, possible to condense useful conclusions from this review for the law of global digitality ("cyberlaw") in general and IP law in particular.

44 Firstly, this article confirms but also qualifies the widely held assumption that code is the dominant mode of cyberspace regulation.[115] It is true that all effective forms of

---

'Geoblocking in EU Copyright Law: Challenges and Perspectives' (2020) 69 GRUR International 136.

[112] See Axel Metzger (ed), *Free and Open Source Software (FOSS) and other Alternative License Models* (2016).

[113] German Federal Court of Justice, case I ZR 69/08, openJur 2010, 528, paras 36 et seq (commercial picture search implicitly authorized); CJEU Case C-466/12, *Nils Svensson v Retriever Sverige AB* ECLI:EU:C:2014:76, paras 23 et seq (hyperlinks).

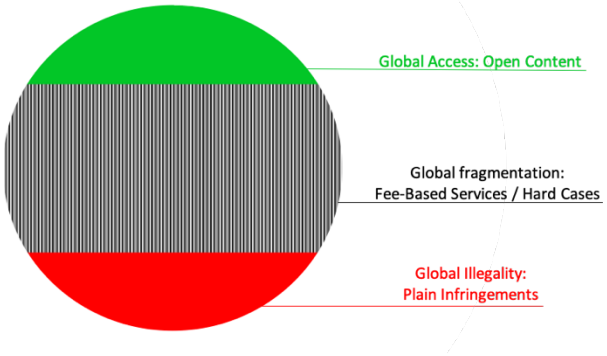
[114] On this distinction see Alexander Peukert, 'Copyright and the Two Cultures of Online Communication' in Paul LC Torremans (ed), *Intellectual Property Law and Human Rights*, (4th ed, 2020) 387.

[115] Cf Lawrence Lessig, *Code and Other Laws of Cyberspace* (1999) 3-60; Reidenberg (n 28), 554–55; Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (2015) 214-5 (legal protection by design).

regulating online communication are executed via software. In some cases examined herein, the functionality of the code also has an impact on the geographical scope of the measure. Thus, domain name cancellations necessarily have global effects, whereas the blocking of a website by an access provider can only affect its customers all of whom reside in a certain region. But if code can be implemented either globally or locally, technology is not determinative as to the geographical scope of IP policies online. Host providers such as Facebook and YouTube operate with service-wide and geographically targeted IP enforcement algorithms at the same time. From a legal point of view, code therefore remains an accessory tool.[116]

45 Secondly, the article demonstrates that private ordering is the primary mode of transnational IP governance on the Internet.[117] Aside of quantitatively insignificant and legally dubious takedown orders of courts with de facto global effects, all instances of transnational IP regulation have been found to be based upon "voluntary" self-regulation by private actors, namely right holders and various intermediaries. Only if and in so far as these actors are willing to execute their rights or their control with regard to Internet infrastructure in a cross-border manner will the territorial fragmentation of IP law be overcome. At the same time, states step back into the nevertheless important role of a facilitator, in whose shadow private actors define their online IP policies.

46 Finally and most importantly, this article brings to light three layers of global Internet governance in the area of IP, which can be represented graphically like this:



[116] Hildebrandt (n 115) 214-5.
[117] Joel R Reidenberg, 'Governing Networks and Rule-Making in Cyberspace' (1996) 45 Emory LJ 911, 921; Monroe E Price and Stefaan G Verhulst, *Self-Regulation and the Internet* (2004) 10-22; Niva Elkin-Koren and Eli M Salzberger, *The Law and Economics of Intellectual Property in the Digital Age* (2013) 149-182.

47 The green layer on the top concerns Open Content, which is subject to a global norm, namely its free accessibility irrespective of the locus of the right holder, the user and any intermediary involved. The red layer on the bottom also depicts a global norm, this time the illegality of plain IP infringements on a commercial scale. It includes the cancellation of domain names registered by "cybersquatters" not having any rights or legitimate interests in respect of the domain name; the blocking of websites not containing a substantial amount lawful information; takedowns of apparently infringing uploads and search results; the blacklisting of websites for advertising purposes whose primary purpose is to infringe; and the termination of payment accounts of "rogue" merchants selling counterfeit or pirated goods.[118] The intermediate layer pertains to licensed, fee-based services and hard cases of conflicts of IP laws/rights. In these markets and legal disputes, territorial fragmentation and thus shades of grey reign.

48 The fact that the three modes of communication and regulation prevail worldwide indicates that they enjoy a high level of legitimacy. The Open Content layer and the market layer derive their legitimacy from the worldwide recognition of IPRs as territorially limited, private rights. 164 WTO and 193 WIPO member states share the view that it is, as a rule, up to the right holder to decide who may use protected IP, under which conditions, and where. If that person finds it proper to grant all Internet users free access to its IP or if she, alternatively, prefers to employ geo-blocking technologies and sell digital goods in certain markets only, so be it. Under the concept of private property, both decisions are equally legitimate. It follows that IP and other laws affecting global digitality should not distort the equilibrium between the open, participative Internet (green layer) on the one hand and fragmented markets for IP (grey layer) on the other by threatening the very existence of any of these cultures of communication.[119]

49 More contentious is the legitimacy of global enforcement measures against cybersquatters, counterfeiters, pirates and other "rogue" actors. From an IP perspective, the extraterritorial reach of cancellations, takedowns and blockings, which are

[118] Supra II 2 b.
[119] Peukert (n 114) 414.

supported only by one or few possibly unspecified IP laws, is problematic.[120] Self-regulatory procedures with worldwide effects also raise concerns as regards their lack of transparency and the difficulty to attribute responsibility to the private and public actors involved.[121] It is feared that far-reaching measures like website blocking can lead to "privatized censorship of online material and other interferences with fundamental rights without a clear legal way of redress or appropriate safeguards such as due process".[122] False positives indeed occur, in particular in the course of billions of host provider and search engine takedowns.[123]

50 In contrast, several self-regulatory IP policies targeting cybersquatters, counterfeiters, pirates or rogue merchants acting on a commercial scale have been smoothly operating for years without producing many complaints about false positives.[124] This fact indicates that the regimes in place are supported by a "rough" global consensus, which is generally sufficient for transnational cyberlaw.[125] And indeed, effectively all states agree that making a current motion picture available on the Internet or selling a product under a well-known trademark without the authorization of the respective right holders is illegal.[126] Regarding "copyright piracy on a commercial scale" and "wilful trademark counterfeiting", Art. 61 TRIPS even obliges all WTO members to provide for criminal procedures and penalties including imprisonment and/or monetary fines sufficient to provide a deterrent. In light of this international law *acquis*, private global enforcement measures against hardcore IP infringements also appear acceptable.

---

[120] Peukert (n 3) 189-228; Trimble (n 11) 541.
[121] Hugenholtz (n 28) 319 ("democratic deficit"); Derek E Bambauer, 'Against Jawboning' (2015) 100 Minn L Rev 51, 60–61; Perel and Elkin-Koren (n 21); Bloch-Wehba (n 29) 79. But see Perlmutter (n 108) 67–68 (arguing that "the long-term future may be in the direction of more general principles in public rules, with more nimble and detailed adaption of those principles through private ordering").
[122] Angelopoulos and others (n 83) 2; Maria Lillà Montagnani, 'Virtues and Perils of Algorithmic Enforcement and Content Regulation in the EU - A Toolkit for A Balanced Algorithmic Copyright Enforcement' (2020) 11 Case W Reserve JL Tech & Internet 1, 28 et seq.
[123] Cf *Lenz v Universal Music Corp* 801 F 3d 1126 (9th Cir 2015); Bar-Ziv and Elkin-Koren (n 67); Toni Lester and Dessislava Pachamanova, 'The Dilemma of False Positives: Making Content Id Algorithms More Conducive to Fostering Innovative Fair Use in Music Creation' (2017) 24 UCLA Ent L Rev 51.
[124] Supra n 39 (UDRP court reviews); European Commission (n 64) 26-7 (setting out the need to provide internal complaint-handling systems).
[125] Callies and Zumbansen (n 43).
[126] Trimble (n 11) 540-1.