Location, location, location! Copyright content moderation at non-content layers

Schwemer, Sebastian Felix

Published in:
Handbook of European Copyright Law

Publication date:
2020

Document version
Early version, also known as pre-print

Citation for published version (APA):
Schwemer, S. F. (2020). Location, location, location! Copyright content moderation at non-content layers. Manuscript submitted for publication. In E. Rosati (Ed.), *Handbook of European Copyright Law* Routledge.

– *Forthcoming as Chapter 17 in: Rosati, E. (2021). Handbook of European Copyright Law, Routledge.* –

Location, location, location! Copyright content moderation at non-content layers

Sebastian Felix Schwemer[*]

Forthcoming as Chapter 17 in: Rosati, E. (2021). *Handbook of European Copyright Law*, Routledge.

ABSTRACT

In the moderation and enforcement of copyright content, online platforms as well as internet access service providers play a prominent role. This contribution looks at less prominently addressed "layers" of the internet, namely in relation to the addressing system in form of domain name system (DNS). It first looks at the functioning of the DNS and its location within the content blocking landscape, before contrasting the DNS with linking, which is well-explored in the copyright jurisprudence and literature, in order to shed light on the role of the DNS in relation to copyright-infringing material. It then turns towards the liability exemption regime of the E-Commerce Directive and the cases of IP address rental and DNS-based content delivery networks. Finally, it looks at the practical role of registration data in the enforcement of copyright and scarce information on "voluntary" arrangements at the DNS-level. The "location" layer of the internet is, compared to online platforms, "far" from copyright-infringing content. Currently, the public consultation in connection with the ongoing review of the E-Commerce Directive under the working title Digital Services Act is touching upon the DNS space. Traditionally, the DNS has not featured prominently in copyright-enforcement debates and it would be wrong to see a prominent role for the DNS going forward. Whereas the "location" layer might be appealing for enforcement purposes, issues and concerns of DNS blocking are manifold and can have serious repercussions on fundamental rights. Yet, already today, there exist voluntary arrangements for the moderation or enforcement of copyright content and the current discussions around the Digital Services Act might be the right place to expand transparency and accountability principles beyond the well-discussed platform enforcement also in the less visible layer of voluntary moderation or enforcement at the "location" layer.

INTRODUCTION

In the context of injunctions and copyright-protected works, the InfoSoc Directive[1] noted in recital 59 already twenty years ago that "[i]n the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities". It continues that therefore "[i]n many cases such intermediaries are best placed to bring such infringing activities to an end." Given the vast developments of the internet over the last two decades, this statement indeed aged well.

[*] Associate Professor, Centre for Information and Innovation Law (CIIR), University of Copenhagen. E-mail: sebastian.felix.schwemer@jur.ku.dk. ORCiD: https://orcid.org/0000-0003-4326-9328.

[1] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, p. 10–19.

Much of the scrutiny around the online enforcement of copyright-protected works focusses on the role internet access service providers, i.e. the telecommunications providers providing end-users with internet access and providing part of the physical infrastructure of the internet[2], or on online platforms such as Facebook, YouTube, Pinterest and others. The practical importance of these intermediaries in the enforcement of copyright has led to ample case law as well as academic writing.

In this chapter, I focus on less prominently addressed aspects of the "logical" layer[3] of the internet, namely the role of the domain name system (DNS).[4] The DNS, as well as the respective intermediaries/service providers, have historically–while not completely off the radar– been somewhat less visible than their internet access service provider or platform counterparts in copyright-related discussions.

This chapter first provides a brief overview of the DNS and its location within the blocking landscape. Then it turns towards the functioning of these more technical intermediaries, before looking at the regulatory landscape. The role of intermediaries in the enforcement of rights can be defined by different factors. The legislative framework in form of liability rules, available injunctions and available liability exemptions with their conditions (such as notice-and-action regimes) provides the basis for the room of operations. This is complemented by a second strain of more or less "binding"[5] rules that further define the governance of intermediaries. These can either be encouraged by or induced by regulators e.g. by non-binding sets of recommendations.[6] Furthermore, also industry self-regulation or best practices play an important role in the governance of intermediaries. Finally, on the individual corporate level, practices, regularly formalized in terms of services, further refine the regulatory environment for how copyright-infringing material is dealt with by intermediaries.

FUNCTIONING OF THE DNS AND ITS LOCATION WITHIN THE CONTENT BLOCKING LANDSCAPE

The DNS forms an essential part of internet infrastructure. In the cybersecurity context and the operation of essential services, the DNS is defined as "hierarchical distributed naming system in a network which refers queries for domain names" in Article 4 No 14 of the NIS

[2] And related to this the provision of Wi-Fi, see C-484/14 *McFadden*, EU:C:2016:689. In Denmark, according to information from the industry organisation *Teleindustrien*, for example, by October 2018 a total of 315 websites have been blocked.

[3] Riordan (2016) differentiates five sub-classes of so-called network layer services, that is services that "route data packets between IP addresses on the internet and supply ancillary services", namely: internet service providers, cloud services, domain name controllers, and certificate authorities, see Riordan, J. (2016). *The Liability of Internet Intermediaries*. Oxford University Press, p. 38 f.

[4] It is important to note that this layer-distinction does not necessarily correspond to existing layer-models in the technical community.

[5] On the notion "non-binding" see below.

[6] In the context of hosting platforms, see e.g. Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, C/2018/1177, *OJ L 63, 6.3.2018, p. 50–61*. In addition, also several Communications by the European Commission contain impulses or calls for self-regulation.

Directive.[7] The DNS is a distributed database and it basically turns numeric Internet Protocol (IP) addresses into user-friendly domain names thereby acting as road signs of the internet.[8] In other words, the DNS "resolves" the domain name into the IP address, e.g. of a server which hosts the website (importantly, multiple websites can be hosted on a single server and thereby be accessible by the same IP address). The naming system is hierarchical and when a domain name is looked up, a query is sent to a root name server to start an iterative process that will end up with a query to a name server that returns an IP address for the specific domain name.

There are a variety of functions and service providers involved in the provision of the DNS. A domain name system service provider is in Article 4 No 15 of the NIS Directive tautologically defined as "an entity which provides DNS services on the internet". A top-level domain name registry is defined in Article 4 No 16 of the NIS Directive "an entity which administers and operates the registration of internet domain names under a specific top-level domain (TLD)". The German country-code top-level domain <.de>, for example, is administered by DENIC, whereas the generic top-level domain <.com> is administered by Verisign. In order to translate or resolve domain names to IP addresses, internet services rely on DNS resolvers, which historically have been operated by internet access service providers.[9] Over the last decade, however, the market for DNS resolving has become significantly more dynamic with the operation of public DNS resolvers, regularly offered free of charge, by e.g. Google, Oracle or Cloudflare.[10]

When we ask the question on what role the DNS and other non-hosting infrastructure-related services of the "location layer" play in copyright enforcement, it is helpful to briefly locate DNS-based actions in the content blocking[11] landscape. There exists a variety of different content and website blocking techniques, which each come with technical and policy limitations and consequences.[12] In the DNS landscape generally much of the debate as well as measures are associated with "technical abuse"[13], i.e. the response to cybersecurity threats where the

[7] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30.

[8] See e.g. Bygrave, L., Schiavetta, S., Thunem, H., Lange, A. B., & Phillips, E. (2009). The naming game: governance of the Domain Name System. In L. Bygrave & J. Bing (Eds.), *Internet Governance: Infrastructure and Institutions* (pp. 147–212). Oxford: Oxford University Press.

[9] Roxana Radu R., & M. Hausding (2020). Consolidation in the DNS resolver market – how much, how fast, how dangerous?, *Journal of Cyber Policy*, 5:1, p. 46.

[10] Ibid. with a critique of the concentration of recursive DNS services. See also Nordemann, J.B. (2020). *The functioning of the Internal Market for Digital Services: responsibilities and duties of care of providers of Digital Services*, Study Requested by the European Parliament's committee on Internal Market and Consumer Protection (IMCO), p. 32.

[11] Conceptually and technically, there is potentially a difference between "blocking" and "filtering". RFC 7754 on "Technical Considerations for Internet Service Blocking and Filtering" explains: "'Blocking' often refers to preventing access to resources in the aggregate, while 'filtering' refers to preventing access to specific resources within an aggregate. Both blocking and filtering can be implemented at the level of 'services' (web hosting or video streaming, for example) or at the level of particular 'content. (...)", see Internet RFC 7754, "Technical Considerations for Internet Service Blocking and Filtering.", March 2016, https://tools.ietf.org/html/rfc7754, p. 4.

[12] Notably, in the United States, DNS blocking was proposed Stop Online Piracy Act (SOPA) and Protect IP Act (PIPA).

[13] See on technical abuse, Schwemer, S. F. (2020). The regulation of abusive activity and content: a study of registries' terms of service. *Internet Policy Review*, *9*(1). DOI: 10.14763/2020.1.1448 and Mahler, T. (2019). *Generic Top-Level Domains; A Study of Transnational Private Regulation*. Edward Elgar, p. 252.

respective services are e.g. used for a distributed denial-of-service (DDoS) attack. Historically, DNS blocking or DNS filtering, was introduced to combat spam e-mails being sent from malicious IP-addresses. The goal of the enforcement of copyright-protected works (and similarly infringements of other rights, e.g., in relation to hate speech, child sexual abuse material or pharmaceuticals[14]), on the other hand, is regularly to make the respective infringing content unavailable. In this context, the goal of a domain-name related measure, for example, is typically that the copyright infringing content can no longer be used to access the respective website.[15] There exist established mechanisms for the blocking or modification of resolution of a domain name for reasons related to the domain name *as such*, e.g. ICANN's Uniform Dispute Resolution Policy (UDRP). Related to the content to which a domain name "links", however, the picture is more complex.

Given its properties and functioning, the directory service provided by the DNS can be used to filter or block access to content or to redirect the end-user e.g. to the nearest content delivery network (CDN).[16] Effectively, DNS blocking breaks the fundamental logical infrastructure of the internet. This is what makes the DNS an appealing but highly problematic layer of internet infrastructure in the enforcement of content.[17] This can be done at different levels. At the client-side web browser level, for example, some web browsers such as Google Chrome and Firefox prevent users from accessing malicious websites by relying on URL blacklist services.[18] These, however, are not subject to the present inquiry.

As already seen from this brief description, the DNS is a relatively complex part of the internet and I will not go further into the many details here. Suffice it to note that DNS service providers are not intermediaries in the transmission of content. However, their service is essential for connecting end users to content providers.

A COPYRIGHT TWIST: DOMAIN NAMES AND THE DNS AS A CASE OF "LINKING"?

Generally, there exists only scarce case law on the liability of domain registries and registrars in relation to content, which I have explored elsewhere.[19] Suffice it here to note that, whereas depending on national secondary liability concept, it cannot be precluded that such DNS actors could be held liable for website content, it is rather unconvincing to hold so given the technical properties of the DNS and its actors noted above.

---

[14] In the context of e-mail spam and domain blacklisting regarding unlicensed prescription pharmaceuticals sites, see e.g. Chachra, N., et al. (2014, June). Empirically characterizing domain abuse and the revenue impact of blacklisting. In *Proceedings of the Workshop on the Economics of Information Security (WEIS)* (Vol. 4).

[15] DeNardis, L. (2012). Hidden levers of Internet control: An infrastructure-based theory of Internet governance. *Information, Communication & Society*, *15*(5), 720–738; p. 728; Schwemer, S.F. (2018). On domain registries and unlawful website content: Shifts in intermediaries' role in light of unlawful content or just another brick in the wall? *International Journal of Law and Information Technology*, *26*(4), 273-293, p. 277.

[16] See in detail below.

[17] Domain name seizures, for example, have generally attracted criticism. See, e.g., Internet RFC 7754, "Technical Considerations for Internet Service Blocking and Filtering.", March 2016, https://tools.ietf.org/html/rfc7754, p. 6 ff.

[18] See, e.g., Google Safe Browsing, https://safebrowsing.google.com or StopBadware https://www.stopbadware.org.

[19] Schwemer, S.F. (2018). On domain registries and unlawful website content: Shifts in intermediaries' role in light of unlawful content or just another brick in the wall? *International Journal of Law and Information Technology*, *26*(4), 273-293.

This said, conceptually the function of a domain name could from its outset be seen as somewhat resembling linking. At first glance, this may appear a far-fetched comparison, but it may nonetheless provide a useful exercise to contextualize the role of the DNS vis-à-vis the – from a copyright-perspective– more extensively analyzed role of hyperlinks (see also the discussion in Chapter 8): when you enter a domain name into a web browser, the domain name is resolved and turned into the numeric IP-address under which the respective "content" is available. Thus, an interesting question to explore is whether DNS-related activities could be seen as falling under the communication to the public right contained in Article 3 of the InfoSoc Directive.[20] If that were the case, various DNS actors, such domain registries and registrars as well DNS-resolvers[21], could potentially be held liable for copyright infringement.

According to established case law, the concept of communication to the public includes two cumulative criteria, namely an act of communication and the communication of that work to a new public. With regard to hyperlinking to copyright-protected material from websites, the Court of Justice of the European Union (CJEU) has established a sophisticated and complicated line of the copyright-relevance of linking in the seminal cases C-466/12 *Svensson*, C-348/13 *BestWater*, and C-160/15 *GS Media*.[22] In *Svensson*, the Court basically established that hyperlinking to copyright protected works which are already freely and lawfully available does not constitute a "communication to the public" because it does not address a new public. This view was reiterated in the *BestWater* case which concerned the scenario of framing and embedded videos. *GS Media*, related to content that is freely available on the internet but without the prior authorization of the relevant rightholder. In that case, the Court was asked "whether, and in what possible circumstances, the fact of posting, on a website, a hyperlink to protected works, freely available on another website without the consent of the copyright holder, constitutes a 'communication to the public' within the meaning of Article 3(1) of Directive 2001/29."[23]

Interestingly, Advocate General (AG) Wathelet suggested in his Opinion – contrary to the Court's findings in *Svensson* – that "[a]lthough it is true that hyperlinks posted on a website make it much easier to find other websites and protected works available on those websites and therefore afford users of the first site quicker, direct access to those works, I consider that hyperlinks which lead, even directly, to protected works do not *'make available'* those works to a public where the works are already freely accessible on another website, but merely

[20] This part of the chapter is inspired by a conversation with Tobias Mahler.
[21] E.g. offered by Verisign, Google, AKAMAI or Cloudflare.
[22] C-466/12 *Svensson*, EU:C:2014:76; C-348/13 *BestWater*, EU:C:2014:2315; C-160/15 *GS Media*, EU:C:2016:644. This chapter does not further look at C-527/15 *Filmspeler*, EU:C:2017:300, which regarded inter alia links to unlawful streaming content and Ziggo, which concerned magnet links: see Jütte, B.J. (2016). "A link too far: CJEU rules that sale equals communication and streaming from unlawful sources is illegal (C-527/15, Filmspeler)", available at https://europeanlawblog.eu/2017/05/24/a-link-too-far-cjeu-rules-that-sale-equals-communication-and-streaming-from-unlawful-sources-is-illegal-c-52715-filmspeler/ (last accessed 1 August 2020). For an in-depth analysis of the *GS Media* case, see Radosavljev, P. (2017). For whom the copyright scale tips: has the CJEU established a proper balance of rights with its GS media case judgement?. *European Journal of Law and Technology*, *8*(3) and Rosati, E. (2017). GS Media and its implications for the construction of the right of communication to the public within EU copyright architecture. *Common Market Law Review*, *54*(4).
[23] *GS Media*, para. 25.

facilitate the finding of those works."[24] The Court did not follow the AG's suggestion. It held instead that Article 3(1) of the InfoSoc Directive

> must be interpreted as meaning that, in order to establish whether the fact of posting, on a website, hyperlinks to protected works, which are freely available on another website without the consent of the copyright holder, constitutes a 'communication to the public' within the meaning of that provision, it is to be determined whether those links are provided without the pursuit of financial gain by a person who did not know or could not reasonably have known the illegal nature of the publication of those works on that other website or whether, on the contrary, those links are provided for such a purpose, a situation in which that knowledge must be presumed.[25]

In other words, the provision of a hyperlink from a website to a copyright work that is freely available but was published without the rightsholder's consent can –at certain conditions– constitute a "communication to the public" within the meaning of Article 3(1) of the InfoSoc Directive.[26]

Already from the outset, these cases are quite distinct and need to be differentiated from a DNS perspective: *GS Media* concerned linking to previously unpublished copyright-protected pictures of Dutch *Playboy*, which were available on an Australian website. Furthermore, the CJEU cases concerned liability of the person posting a link. Transferred to the DNS, this would be the registrant, who regularly is the actor that also makes the hosted content available. Other DNS actors, such as e.g. registries or registrars, however, could merely fall under contributory liability according to the respective national concepts (i.e. used as an accessory of the registrant).[27]

Despite these differences, there are a couple of transferable thoughts, however, which help shed light on the role of the DNS in relation to copyright-infringing material. Notably, the Court in *GS Media* pointed towards the importance of the internet for the exercise of fundamental rights and the central role of hyperlinking commenting that

> the internet is of particular importance to freedom of expression and of information [...], and hyperlinks contribute to its sound operation as well as to the exchange of opinions and information in that network characterised by the availability of immense amounts of information.[28]

---

[24] Opinion AG Wathelet, EU:C:2016:221, para. 54. See also paras. 55–60, touching inter alia on the indispensable criterion vis a vis mere facilitation of access in *Football Association Premier League and Others* (C-403/08 and C-429/08, EU:C:2011:631) vis-à-vis *SGAE* (C-306/05, EU:C:2006:764, para. 42) and *Svensson and Others* (paras. 27 and 31).

[25] *GS Media*.

[26] The judgement has been interpreted as establishing a *de facto* take-down obligation for users, see e.g. Rosati, E. (2016). "Hyperlinks and communication to the public: early thoughts on the GS Media decision", available at http://ipkitten.blogspot.com/2016/09/hyperlinks-and-communication-to-public.html (last accessed 1 August 2020).

[27] See on contributory / secondary liability in the context of Article 3(1) InfoSoc Directive also Opinion AG Saugmandsgaard Øe in Joined Cases C-682/18 *YouTube* and C-683/18 *Cyando*, EU:C:2020:586, paras. 94 ff.

[28] *GS Media* para. 45. See Opinion AG Wathelet, para. 54. One of the accompanying footnotes (28) reads: "I believe that, because of the enormous quantity of information available on the internet, such information would actually be largely unfindable without hyperlinks. In my view, hyperlinks are at present an essential element of the internet

Given the essential function of domain names in the current architecture of the internet, the same must be said of the DNS.

Furthermore, the Court considered the intricacies of copyright licensing and noted that

> it may be difficult, in particular for individuals who wish to post such links, to ascertain whether website to which those links are expected to lead, provides access to works which are protected and, if necessary, whether the copyright holders of those works have consented to their posting on the internet.[29]

Translating this to the DNS, one can only presume that the difficulty for a party, that not actively connects a domain name to the content available under an IP-address but merely acts as intermediary, is at least as relevant. The Court further continued, noting that:

> [m]oreover, the content of a website to which a hyperlink enables access may be changed after the creation of that link, including the protected works, without the person who created that link necessarily being aware of it.[30]

And indeed, also the very nature of the DNS is that the content available under the IP address as well as the IP address as such can be changed. In fact, one IP address may very well be associated with many different hosting parties.

Admittedly, the comparison between hyperlinking to a copyright-protected work and the various DNS functions in pointing towards IP addresses might be far-fetched. In conclusion, however, it would be surprising – to say the least – if courts were to find a more extensive interpretation of the communication to the public concept in Article 3(1) of the InfoSoc Directive in relation to the DNS than what has occurred in relation to hyperlinking.

LIABILITY EXEMPTIONS IN THE E-COMMERCE DIRECTIVE

Another starting point in order to assess the role of these intermediaries in copyright enforcement, is to look at the applicability of the liability exemption regime in the E-Commerce Directive[31], because it gives us an idea of the conditions that an intermediary needs to satisfy in order to be exempt from (potential) liability. The E-Commerce Directive provides a horizontal liability exemption for certain intermediary functions, namely "mere conduit"[32] (Article 12), "caching"[33] (Article 13) and hosting (Article 14) and comes with certain conditions that the respective information society service provider needs to fulfil in order to benefit from

architecture." In the same sense, see also Opinion AG Saugmandsgaard Øe in Joined Cases C-682/18 *YouTube* and C-683/18 *Cyando*, EU:C:2020:586, para. 241.

[29] GS Media, para. 46.

[30] GS Media, para. 46.

[31] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17.7.2000, p. 1–16.

[32] Note the quotation marks in the Directive.

[33] Note the quotation marks in the Directive.

the liability exemption. The specific conditions of the liability exemptions, in turn, influence the role of these actors.[34]

DNS services and the E-Commerce Directive

When the E-Commerce Directive was adopted over 20 years ago, the EU legislature did not directly address the role of DNS providers in the intermediary liability exemption framework in Articles 12 to 15 of the Directive.[35] Over the years, the CJEU has taken a stance on a variety of service providers and their eligibility for the liability exemptions, including in relation to the provision of WiFi-hotspots[36] and IP address rental[37]. There exists, however, very scarce case law on other functions and actors.[38] In the copyright-enforcement context, the question of liability exemptions arises, for example, when a claimant wants to claim damages from an infringer.

In order to benefit from one of the E-Commerce Directive's liability exemptions, such service needs to fulfil several conditions. First, it needs to be the provider of an information society service. Such service is defined as autonomous concept in Article 1(1) lit. b of the Technical Standards Directive[39], as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services." DNS-services are not directly mentioned but neither contained in the indicative list of excluded services in Annex I of the Directive. While DNS-queries are not normally provided for remuneration, this does not inhibit the qualification as information society service providers because the condition does not require that the service is paid for by those for whom it is performed.[40] Given the broad genus of the information society service provider concept[41], however, the provision of DNS functions is likely falling within this concept. This criterion might, however, be more problematic with regards to registrars which regularly have no control over the DNS as such because it remains with the registry, have no influence on the terms of service for the respective TLD and can be substituted by another registrar.[42] Lower court jurisprudence suggests, that at least domain registries are to be considered information society service providers.[43] Secondly, the activity of such service needs to be "of a mere technical, automatic and passive nature, which implies that

[34] See, e.g., on the developments of notice-and-action regimes under Article 14 E-Commerce Directive.

[35] Domain names are mentioned in Article 2 (f) of the E-Commerce Directive in connection with "commercial communication", which implies that the DNS has not been completely off the radar of the lawmaker.

[36] C-484/14 *McFadden*, EU:C:2016:689.

[37] See further below.

[38] For a non-exhaustive overview of lower court jurisprudence from different Member States in relation to liability and liability exemptions of domain registries and registrars before the *SNB-REACT* case (C-521/17 *SNB-REACT*, EU:C:2018:639), see Schwemer, S.F. (2018). On domain registries and unlawful website content, International Journal of Law and Information Technology, 26(4), pp. 273–293, DOI: 10.1093/ijlit/eay012

[39] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, OJ L 241, 17.9.2015, p. 1–15.

[40] See e.g. *Mc Fadden*, para 43. See earlier Case 352/95, *Bond van Adverteerders*, ECR 1988, 2085, point 16.

[41] See the CJEU's case law on information society service provider notion e.g. in *McFadden*.

[42] Thus, the true nature of a registrar service could be qualified as merely commercial mediation, see e.g. C-434/15 *Uber Spain*, EU:C:2017:981 and C-390/18 *Airbnb Ireland*, EU:C:2019:1112.

[43] Schwemer, S. F. (2018). On domain registries and unlawful website content: Shifts in intermediaries' role in light of unlawful content or just another brick in the wall?. *International Journal of Law and Information Technology*, *26*(4), 273-293.

the information society service provider has neither knowledge of nor control over the information which is transmitted or stored".[44]

Assuming that such intermediary is to be seen as information society service provider, the question is whether DNS- or IP address-related service providers could be read under the current liability exemption. When looking at the intermediary functions addressed in the E-Commerce Directive, however, it becomes clear that they do not fit very well the case for the DNS. I have elsewhere argued that Article 12 of the E-Commerce Directive, given its *raison d'être*, could be applied in a teleological reading or by analogy.[45] *A maiore ad minus*, it makes little sense if intermediary information society service providers that are much closer to content, such as online platforms, can benefit from a liability exemption whereas DNS actors cannot. At the time of writing, however, there exists no reference before the CJEU that would clarify the question, which may be to the detriment of legal certainty. This lack of jurisprudence and of a reference to the CJEU could also be an indicator that the DNS indeed plays a neglectable role in copyright infringements. In any case, there have – despite the seemingly unclear position within the liability exemption framework of the E-Commerce Directive – emerged various responses by DNS actors on the issue, which will be touched upon below.

The case of IP address rental

In the case C-521/17 – *SNB-REACT*, the referring Estonian court asked the CJEU *inter alia* whether "even a service provider whose service consists in registering IP addresses, thus enabling them to be anonymously linked to domains, and in renting out those IP addresses" (para. 26) can fall under the liability exemptions in Articles 12 to 14 of the E-Commerce Directive. The case concerned the enforcement of intellectual property rights, specifically trade mark rights.[46] Given the horizontal nature of the E-Commerce Directive's liability exemption rules, however, the case is also of interest in relation to the role such service providers play in the enforcement of copyright-protected works. The plaintiff, a Belgian anti-counterfeiting network representing trade mark owners in the proceedings, had brought an action seeking an injunction terminating infringement and preventing any future infringements of the trade mark rights in question. It argued that the defendant had registered internet domain names that were used to sell counterfeit goods. While acknowledging ownership over 38,000 IP-addresses, the defendant noted that they were rented out to two third parties and that his services consisted of providing access to an electronic communications network together with an information transmission service.

---

[44] Recital 42 E-Commerce Directive. For hosting in the sense of Article 14 E-Commerce Directive, the CJEU applied the criterion in in C-324/09 *L'Oréal and Others*, EU:C:2011:474, para. 113; C-236/08 to C-238/08 *Google France and Google*, EU:C:2010:159, para. 113; C-291/13 *Papasavvas*, EU:C:2014:2209, paras. 40 ff.; however, not uncontested see e.g. C-324/09 *L'Oréal v eBay*, Opinion of AG Jääskinen, EU:C:2010:757, paras. 138–142.

[45] For a discussion in the academic literature see Schwemer, S. F. (2018). On domain registries and unlawful website content: Shifts in intermediaries' role in light of unlawful content or just another brick in the wall?. *International Journal of Law and Information Technology*, *26*(4), 273-293, with further references; see also: Truyens, M., & Van Eecke, P. (2016). Liability of domain name registries: Don't shoot the messenger. *Computer Law & Security Review*, *32*(2), 327-344.

[46] The national claim had been filed by ten members, including Willy Bogner GmbH & Co. KGaA; Burberry Ltd; FITFLOP Ltd; Franklin & Marshall S.r.l. A socio unico; TM 25 Holding B.V; New Era Cap Cp Inc; Pandora A/S; Ape & Partners S.p.A; Puma AG; TBL Licensing LLC rights protection.

From the judgment, it is somewhat unclear exactly what type of service is being considered and it has been interpreted by some as addressing domain registrars.[47] The CJEU rephrased the referring court's question at para. 40, essentially addressing the "provider of an IP address rental and registration service allowing domain names to be used anonymously". From the context of the case, it seems that the defendant offered only an IP address rental and registration service, which allowed the defendant's "*customers* to use domain names and websites anonymously" (para. 49, emphasis added). Thus, it appears that the defendant indeed only rented out IP addresses but not domain names as claimed by the plaintiff (para. 18). This reading is also confirmed by the preceding Estonian decision, which at para. 17 noted that "[t]he Land Court concluded, as a collection of evidence, that the defendant was only the owner of IP addresses, not the registrar or owner of websites."[48]

In its judgment of 7 August 2018, the Court held that such service, in any case, can fall under the E-Commerce Directive's liability exemptions provided that the relevant criteria are fulfilled.[49] Unfortunately, the CJEU refrained from giving further guidance on whether such service would qualify under "mere conduit", "caching" or hosting, thus leaving it for the referring Court to verify and assess the situation (paras. 50 and 52).[50] Drawing a distinction is of high relevance with a view to the consequences such as notice-and-action requirements set out e.g. in Article 14 E-Commerce Directive. Notably, AG Wathelet refrained from issuing an opinion in the case.[51]

The case of content delivery networks

Since the adoption of the E-Commerce Directive in 2000, the internet has developed from static websites into more dynamic websites with increasing data transmission. In order to facilitate this, content delivery network (CDN) service provider have emerged which geographically distribute the delivery of content. Currently, "DNS-based server redirecting is considered the most popular means of deploying CDNs."[52] In other words, the DNS is used as a means of distributing the requests to different servers. One technical consequence of the use of CDNs is that the IP address of the website owner is no longer visible; instead the IP address of the CDN is returned. The use of CDNs is widespread among both legal and illegal websites and

[47] Some have interpreted the case as being concerned with domain registrars: see, e.g., Allgrove, B. & Groom, J. (2020). Enforcement in a digital context: intermediary liability. In: T. Aplin (Ed.), *Research Handbook on Intellectual Property and Digital Technologies* (pp. 506–530). Edward Elgar, p. 508; Nordemann, J.B. (2020). *The functioning of the Internal Market for Digital Services: responsibilities and duties of care of providers of Digital Services*, Study Requested by the European Parliament's committee on Internal Market and Consumer Protection (IMCO), p. 33.

[48] See Tallinna Ringkonnakohus (date of decision: 26.11.2018, entry into force: 15.01.2019, local case no: 2-14-6942): https://www.riigiteataja.ee/kohtulahendid/fail.html?fid=241007681 [Translation from Estonian using https://neurotolge.ee/)] (last accessed 1 August 2020).

[49] See Rosati, E. (2018). "Has the CJEU quietly changed the conditions for safe harbour availability?", available at http://ipkitten.blogspot.com/2018/08/has-cjeu-quietly-changed-conditions-for.html (last accessed 1 August 2020).

[50] See also C-521/17, *SNB-REACT*, EU:C:2018:639, para. 42.

[51] This could be interpreted as to the straight-forward character of the referred question or the case's minor importance. But also *Svensson* and *BestWater* were rendered as Judgment and Order respectively without a prior opinion of the appointed AG.

[52] Wang, Z., Huang, J., & Rose, S. (2018). Evolution and challenges of DNS-based CDNs. *Digital Communications and Networks*, *4*(4), 235-243.

the role of these intermediaries has recently been challenged by copyright rightsholders in European lower courts.[53] The following two cases illustrate some of the issues at stake:

In a first case, on 13 March 2019, Cloudflare was ordered by the Rome Court of First Instance in proceedings for a preliminary injunction to terminate the account of "several pirate websites".[54] In the Italian *Cloudflare* case, it was held that the service falls in principle under the E-Commerce Directive.[55] By focussing on the hosting element of the service and leaving aside the caching and mere conduit activities, the result was that Cloudflare failed to fulfil the condition in Article 14 E-Commerce Directive and the Italian corresponding provisions and "[t]herefore, there arises liability of the resistant for both the collaboration in the spread of audio-visual files over which the plaintiff holds exclusive rights of economic exploitation [...] and carrying out of the hosting provider activity".[56] This decision does not bring much clarity regarding the "location" part, but there are currently several further full-motion proceedings pending in Italy, which might shed more light on CDN's setup in general and potentially the role of this specific use of the DNS within the E-Commerce Directive.

Another recent German lower jurisprudence case before the District Court of Cologne also concerned Cloudflare.[57] The case related to an injunction regarding the website <ddl-music.to>, where various hyperlinks offered by various filesharing platforms to a music album were made available without the permission of rightholder Universal. In the case, the plaintiff argued that the CDN provider Cloudflare performed a communication to the public in accordance with CJEU case law, because it continued to keep the infringing content of its customer online despite concrete knowledge of the copyright infringement.[58] The plaintiff argued that the defendant could not rely on the mere conduit liability exemption[59], because it *inter alia* selected the receivers at multiple-stages, as contractual partner of <ddl-music.to>. The plaintiff also requested that Cloudflare cease the DNS-resolver service for <ddl-music.to>.

Cloudflare, on the other hand, argued that it did not provide a hosting service and merely offered the transient storage of content in the sense of Articles 12 and 13 of the E-Commerce Directive.[60] The defendant furthermore declared in lieu of an oath that only specific static content would be temporarily saved on servers, whereas audio- and video-content would be generally excluded because the amount of data is unsuitable for efficiency-raising caching.[61] Thus, the activity would be restricted to the automatic redirection of content, which was

[53] In the US, see e.g. United States District Court Central District of California (case no. CV 16-5051-GW (AFMx). One service provider, Cloudlflare, was in 2018 included in the European Commission's Counterfeit and Piracy Watch List, see European Commission (2018). *Counterfeit and Piracy Watch List*, Brussels, 7.12.2018 SWD(2018) 492 final.

[54] *Mediaset (RTI) v. Cloudflare,* (order of Rome Court of First Instance of 13 March 2019, 1932/2019).

[55] *Mediaset (RTI) v. Cloudflare* (order of Court of Rome VI of 24 June 2019, 26942/2019), p. 2.

[56] *Mediaset (RTI) v. Cloudflare,* (order of Rome Court of First Instance of 13 March 2019, 1932/2019)., p. 12.

[57] *Universal Music GmbH (Germany)*, Cologne District Court (Landgericht Köln) on December 5, 2019, case no. 14 O 171/19.

[58] Ibid., p. 10.

[59] Article 12 E-Commerce Directive implemented in § 8 of the German Telemedia Act (TMG).

[60] Or rather, the German implementation in § 8 and § 9 TMG. *Universal Music GmbH (Germany)*, Cologne District Court (Landgericht Köln) on December 5, 2019, case no. 14 O 171/19, p. 17.

[61] *Universal Music GmbH (Germany)*, Cologne District Court (Landgericht Köln) on December 5, 2019, case no. 14 O 171/19p. 18.

neither chosen nor adapted in its form. Finally, Cloudflare noted that the blocking of specific content available under a specific URL is not possible given the structure of its services and that a complete blocking of <ddl-music.to> would be disproportionate.

Because the name servers of the CDN were used for this function, only Cloudflare's IP-addresses are visible, whereas the IP address of the domain with the infringing content was invisible. Thus, to some extent this situation resembles the Whois-aspects of domain names. In essence, the court had to assess whether the defendant with regard to inter alia the DNS-resolver function was covered by the "mere conduit" liability exemption of Article 12 of the E-Commerce Directive.

The court underlined that the business model of the defendant is not based on the promotion of copyright infringements; rather, the anonymization of IP-addresses is an inevitable technical consequence of the integration of the CDN and thus not intentionally installed to foster the infringement of copyright-protected works.[62] Furthermore, the court confirmed – by relating to the existing German case law on internet access service providers – that the defendant has no duty to monitor or investigate the content of domains, for which it acts as nameserver and CDN server.[63] In relation to a potential liability exemption of Cloudflare, also the German court confirmed that its services would constitute an information society service provider[64] and recalled the conditions of the "mere conduit" liability exemption, noting however that these were not fulfilled in the present case.[65] The court assessed that the service was not restricted to the mere automatic storage.[66] Rather, Cloudflare was deemed, on the basis of its contract with its clients, to intervene in many dimensions in the transmission of information between users and website owners.[67] Notably, the defendant – and not the website owner– was argued to be involved in the selection of addressees of the transmitted information by filtering or sorting a part of the users based on the requesting IP-address.[68] Furthermore, the court noted that not only the intermediate, transient storage of website content is taking place, but rather as much as possible is stored on the local servers of the CDN.[69] . The service aimed at the optimization and acceleration of the website that was performed by Cloudflare as name server via its CDN, so the court did argue, was necessarily coming with interventions in the transmission of information from and to the website of its customers, partly because Cloudflare guaranteed the availability of the customer's website even if it is temporarily inaccessible. Thus, the Court considered that Cloudflare would not be a "neutral" (passive) service provider in the sense of Article 12 E-Commerce Directive, i.e. merely performing the intermediate storage with the purpose of acceleration of transmission of information. In essence, *Cloudflare*

[62] *Universal Music GmbH (Germany)*, Cologne District Court (Landgericht Köln) on December 5, 2019, case no. 14 O 171/19, p. 29. In fact, services like Cloudflare are relied on by many websites. Despite this, however, *Cloudflare* was included in the European Commission's Counterfeit watch list, see above.
[63] Ibid., p. 29.
[64] Ibid., p. 27.
[65] Ibid..
[66] Ibid.
[67] Ibid.
[68] Ibid., p. 28.
[69] Ibid. The court saw this substantiated in the fact that, if a website is temporary unavailable, Cloudflare presented this content from its own servers, which "unavoidably" means the selection and adaptation of content.

selected which users get access to the website and did "not only do transient copies, but retains content provided by the customers on different local servers."[70]

It is important to note that both the examples discussed above regard preliminary injunctions before lower courts[71] and they do not provide a clear answer to the question of where to locate CDNs within the E-Commerce framework. Yet, both cases also illustrate the difficulty of one specific use of the DNS (in this instance as a "hack" for distributing requests to CDN servers) within the E-Commerce Directive.

INFORMATION ABOUT THE INFRINGER: THE PRACTICAL ROLE OF REGISTRATION DATA

Domain registries and registrars provide another important resource for rightholders in the enforcement of copyright: the Whois database, which provides a domain name registrant's contact information. Importantly, Whois is not a single centralized database; instead, it is run and maintained by either the respective registry or registrar.[72] While tracing back to ARPANET in 1982, it has developed into an important tool for rightholders, law enforcement and users alike. Similarly, the RIPE database provides certain Whois information for IP addresses.[73]

Access to this information can be relevant for enforcement purposes when identifying infringing parties.[74] Yet, this access needs to be balanced *inter alia* again the protection of personal data. In the context of the Enforcement Directive[75], the CJEU recently held that Article 8 on the "'Right of information" in the Enforcement Directive "does not cover, in respect of a user who has uploaded files which infringe an intellectual property right, his or her email address, telephone number and IP address used to upload those files or the IP address used when the user's account was last accessed."[76] In connection with the GDPR, the practices around Whois databases of domain registries have changed.[77] In the context of gTLDs, the ICANN community is currently drafting a "System for Standardized Access/Disclosure to non-public gTLD registration data ('SSAD')", which is currently in the public comment period.

Registration data is also *one* angle for proactive "voluntary" measures related to (copyright) infringing activities. Some domain registries have identified a plausible correlation between

[70] Nordemann, J.B. (2020). *The functioning of the Internal Market for Digital Services: responsibilities and duties of care of providers of Digital Services*, Study Requested by the European Parliament's committee on Internal Market and Consumer Protection (IMCO), p. 33.

[71] Additionally, the German judgment is surprisingly packed with grammatical errors and spelling mistakes.

[72] See description by ICANN, available at https://whois.icann.org/en/about-whois#field-section-1 (last accessed 1 August 2020).

[73] See e.g. https://apps.db.ripe.net/db-web-ui/query (last accessed 1 August 2020).

[74] At the same time, it is important to note that –looking beyond copyright– many "abused" domain names are legitimate domain names that get compromised.

[75] Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30.4.2004), OJ L 195, 2.6.2004, p. 16–25.

[76] C-264/19 *Constantin Film,* EU:C:2020:542, para. 40 See also C-275/06 *Promusicae*, EU:C:2008:54, paras 45 and 70; C-557/07 *LSG*, EU:C:2009:107, para 29; as well as: C-461/10 *Bonner Audio,* EU:C:2012:219; and C-149/17 *Bastei Lübbe,* EU:C:2018:841.

[77] In Denmark, pre-existing national legislation has mitigated this issue of Whois for the national ccTLD to a certain extent.

domain names that are used for unlawful purposes and the quality of the registration data and introduced data validation processes.[78] In order to register a <.dk>-domain name, for example, Danish citizens need to validate their registrant information by using the common log-in solution NemID, which is used by, e.g., banks and the public sector. Generally, however, such measure depends on the existence of identity validation systems. This focus on registration data quality is appealing, given that it potentially constitutes a practical solution to the practical problem of using a domain name in connection with infringing content, without having the intermediary to perform an assessment of content. Importantly, the desired outcome – i.e. a reduction of domain names being used for making copyright-protected works available without rightholders' consent – is merely a by-product of ensuring correct registration data.[79] Registrants, however, might have a legitimate interest not to register a domain name under their name. This could be, for example, the case if a registrant feared repercussions, e.g., in connection with political speech. And whereas this example has nothing to do with copyright, it shows that debates on copyright enforcement cannot ignore potential effects on non-copyright related aspects.

"VOLUNTARY" ARRANGEMENTS

Finally, there exists a self-regulatory reality outside – but not entirely detached from – the legislative intervention. The question of what constitutes "voluntary" measures or arrangements largely depends on what service providers are obliged to undertake regarding usage of their services for copyright-infringing material, i.e. their liability.[80] The motivations for this form of self-regulation can be manifold, ranging from altruistic motives or CSR concerns to the management of legal risks.

Despite their seemingly unclear role in the liability exemption regime, some DNS intermediaries have engaged in a variety of arrangements regarding the enforcement of illegal content and – a certain degree – copyright. A first aspect relates to the service providers' terms and conditions with their respective customers.[81] A domain registry or CDN service provider may reserve the right to cancel the service agreement with its customer under certain conditions. In 2017, Cloudflare, for example, dropped DDoS-attack protection for the right-wing website The Daily Stormer as a customer, following the lead of other intermediaries including Google given public pressure against the provision of services to the website. Generally, it appears rare that intermediaries address copyright-infringements somehow related to their activities on their own initiative. Instead, there exist several examples of collaboration between a service provider and

[78] E.g. Nominet, DK Hostmaster, DNS Belgium, EURid: see Schwemer, S.F. (2020). The regulation of abusive activity and content: a study of registries' terms of service. Internet Policy Review, 9(1).

[79] Registries will regularly not perform an analysis of content to which the domain name links.

[80] In the context of hosting, i.e. online platforms, the question of whether certain platforms themselves carry out a relevant act of communication to the public according to Article 3(1) of the InfoSoc Directive in addition to the users' copyright-relevant actions, there are currently two pending references for a preliminary ruling by the German Bundesgerichtshof before the CJEU, namely case C-682/18 - *YouTube* and case C-683/18 - *Elsevier*. The direct liability for online content sharing service providers comprising e.g. Youtube or Instagram, a subgroup of information society service providers, in Article 17(1) of the DSM Directive.

[81] In the context of ccTLD registries, see Schwemer, S.F. (2020). The regulation of abusive activity and content: a study of registries' terms of service. *Internet Policy Review*, 9(1) and for gTLDs Kuerbis, B., Mehta, I., & Mueller, M. (2017). *In Search of Amoral Registrars: Content Regulation and Domain Name Policy*. Atlanta: Internet Governance Project, Georgia Institute of Technology.

a so-called "trusted notifier". In relation to online platforms, a trusted notifier (also referred to as trusted flagger or trusted reporter) is defined in the European Commission's Recommendation on measures to effectively tackle illegal content online as "an individual or entity which is considered by a hosting service provider to have particular expertise and responsibilities for the purposes of tackling illegal content online".[82] The Commission bases its recommendation on the assumption that such arrangements lead to "higher quality notices and faster take-downs" vis-à-vis traditional notice-and-action regimes.[83]

Similar arrangements can also be traced in the DNS environment.[84] Counterintuitively an empirical study found that the reputation of notifiers made no difference in the action taken by DNS intermediaries.[85] There exist, for example, several gTLD[86] and ccTLD[87] registries that have trusted-notifier akin regimes in place. According to the German *Cloudflare* case, also the CDN provider Cloudflare maintains a trusted-reporter programme with the Recording Industry Association of America (RIAA).[88] These arrangements do, however, not come without concern[89], *inter alia* because the risk of rubberstamping and the risk for over-removal in the case of false positives. Concerns are aggravated by the fact that there often exists little transparency into the workings of these arrangements. Given the changes in the availability of Whois information, these models might become more important in the future.

MAKING SENSE OF "LOCATION" IN THE ENFORCEMENT OF COPYRIGHT

The primary interest of a copyright holder is to stop the infringing activity. The liability exemption regime, briefly touched upon above, does not restrict rightholders' access to injunctions.[90] Thus, provided that the existence of an infringement or risk of infringement of copyright has been established in accordance with the respective legal standard, "a targeted measure intended to bring an end to that infringement or to prevent that risk" is still possible.[91] Articles 11 of the Enforcement Directive and 8(3) of the InfoSoc Directive oblige Member States to provide for injunctive relief, which regularly is the practical interest of rightholders (see the discussion in Chapter 16). Dynamic blocking injunctions are another development in

[82] Chapter 1, point 4 lit. g of Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online C/2018/1177 [2018] OJ L 63, pp. 50–61. Such setup is foreseen both in relation to private and public actors (competent authorities).
[83] The Commission's Recommendation is also of interest outside the platform space, see recital 15.
[84] See Schwemer, S.F. (2019). Trusted notifiers and the privatization of online enforcement, *Computer Law & Security Review*, 35(6), 105339.
[85] Cetin, O., Hanif Jhaveri, M., Gañán, C., van Eeten, M., & Moore, T. (2016). Understanding the role of sender reputation in abuse reporting and cleanup. *Journal of Cybersecurity*, *2*(1), 83-98.
[86] See for a detailed analysis: Bridy, A. (2017). Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation. *Wash. & Lee L. Rev.*, *74*, 1345.
[87] See Schwemer, S.F. (2019). Trusted notifiers and the privatization of online enforcement, *Computer Law & Security Review*, 35(6), 105339.
[88] Interestingly, there is no public information available on Cloudflare's website.
[89] See for a critique Schwemer, S.F. (2019). Trusted notifiers and the privatization of online enforcement, *Computer Law & Security Review*, 35(6), 105339.
[90] See Articles 12(3), 13(2) and 14(3) of the E-Commerce Directive and: *SNB-REACT*, para. 51; *Mc Fadden*, paras. 77, 78 and 94.
[91] *SNB-REACT*, para 51.

the handling of large scale repeat online –often copyright-related– infringements, for example with regards to mirror-sites, that have been granted in several EU Member States.[92]

In this chapter, I have looked at the role of certain non-hosting intermediaries in the enforcement of copyright infringements. The "location" layer of the internet is, compared to online platforms, far from copyright-infringing content. In the parallel debate involving online platforms, we can witness a shift from the reactive notice-and-action arrangements based on the E-Commerce Directive, towards more a proactive role. The rationale for this, however, cannot simply be stretched into other non-hosting intermediaries such as the DNS space.

Currently, the public consultation in connection with the ongoing review of the E-Commerce Directive under the working title Digital Services Act is also touching upon the DNS space.[93] Any discussion on reasonable expectations for the role of DNS intermediaries, however, needs to be based on what DNS actors actually can do and what the DNS' relation to content is. The DNS has not featured prominently in copyright-enforcement debates and it would be wrong to see a prominent role for the DNS going forward. Besides conceptual challenges, arguments range from the intermediaries, e.g. registries and registrars having very little information, and the extremely low costs of DNS. The "location" layer is appealing for enforcement purposes, but the issues and concerns of DNS blocking are manifold and can have serious repercussions on fundamental rights. Any DNS-related measure must be proportionate, both in concrete copyright-infringement cases as well as in secondary legislation addressing the role of the DNS. There can exist a variety of aims that might qualify as legitimate, including the enforcement of copyright. However, a DNS measure is by default only partly suitable to achieve that aim because it will merely lead to a more limited availability in practice as the content may still be available on host servers via IP addresses.

Already today copyright enforcement at the DNS-level relies on voluntary arrangements and my expectation is that this is likely to increase over time. In this context, it is necessary to stress the need for more transparency into these copyright content "moderation" arrangements in several dimensions. First, information about the existence of such mechanism and its procedure: secondly, substantive information about the criteria; and, thirdly, related to reporting, i.e. what was decided, how and why. Besides transparency, these arrangements should also include procedural safeguards such as the challenging of notices e.g. in-house, via alternative dispute resolution mechanisms or authorities.[94] Recommendation (EU) 2018/334 goes a long way but is primarily addressing platforms and constitutes a non-binding instrument.[95] Similarly, the DSM Directive contains some redress mechanisms, which, however

[92] On the development towards dynamic blocking injunctions see van der Donk, B. (2020). How dynamic is a dynamic injunction? An analysis of the characteristics and the permissible scope of dynamic injunctions under European Law after CJEU C-18/18 (Glawischnig-Piesczek). *Journal of Intellectual Property Law & Practice,* jpaa071.

[93] Available at https://ec.europa.eu/digital-single-market/en/news/consultation-digital-services-act-package (last accessed 1 August 2020).

[94] See, e.g., Uniform Domain-Name Dispute-Resolution Policy (UDRP), URS (Uniform Rapid Suspension).

[95] The Recommendation notes, for example, that "(...) decisions taken by hosting service providers to remove or disable access to content which they store should take due account of the fundamental rights and the legitimate interests of their users as well as of the central role which those providers tend to play in facilitating public debate and the distribution and reception of facts, opinions and ideas in accordance with the law."

are restricted to the online content sharing platform realm.[96] The Digital Services Act might be the right place to make these basic principles binding beyond the well-discussed platform enforcement also in the less visible layer of enforcement at the location-level.

REFERENCES

Bibliography

Allgrove, B. & Groom, J. (2020). Enforcement in a digital context: intermediary liability. In: T. Aplin (Ed.), *Research Handbook on Intellectual Property and Digital Technologies* (pp. 506–530). Edward Elgar.

Bridy, A. (2017). Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation. *Wash. & Lee L. Rev.*, *74*, 1345.

Bygrave, L., Schiavetta, S., Thunem, H., Lange, A. B., & Phillips, E. (2009). The naming game: governance of the Domain Name System. In L. Bygrave & J. Bing (Eds.), *Internet Governance: Infrastructure and Institutions* (pp. 147–212). Oxford: Oxford University Press.

Cetin, O., Hanif Jhaveri, M., Gañán, C., van Eeten, M., & Moore, T. (2016). Understanding the role of sender reputation in abuse reporting and cleanup. *Journal of Cybersecurity*, *2*(1), 83-98.

Chachra, N., McCoy, D., Savage, S., & Voelker, G. M. (2014, June). Empirically characterizing domain abuse and the revenue impact of blacklisting. In *Proceedings of the Workshop on the Economics of Information Security (WEIS)* (Vol. 4), http://www.econinfosec.org/archive/weis2014/papers/Chachra-WEIS2014.pdf

DeNardis, L. (2012). Hidden levers of Internet control: An infrastructure-based theory of Internet governance. *Information, Communication & Society*, *15*(5), 720–738.

Internet RFC 7754 (March 2016). Technical Considerations for Internet Service Blocking and Filtering. https://tools.ietf.org/html/rfc7754

Jütte, B.J. (2016). "Saving the Internet or linking limbo? CJEU clarifies legality of hyperlinking (C-160/15, GS Media v Sanoma)", available at https://europeanlawblog.eu/2016/09/20/saving-the-internet-or-linking-limbo-cjeu-clarifies-legality-of-hyperlinking-c-16015-gs-media-v-sanoma/ (last accessed 1 August 2020)

[96] See Article 17
Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ L 130, 17.5.2019, p. 92–125; Schwemer, S., & Schovsbo, J. H. (2020). What Is Left of User Rights: Algorithmic Copyright Enforcement and Free Speech in the Light of the Article 17 Regime. In: P. Torremans (Ed.), *Intellectual Property Law and Human Rights* (4th edition, pp. 569-589). Alphen aan den Rijn: Wolters Kluwer.

Jütte, B.J. (2016). "A link too far: CJEU rules that sale equals communication and streaming from unlawful sources is illegal (C-527/15, Filmspeler)", available at https://europeanlawblog.eu/2017/05/24/a-link-too-far-cjeu-rules-that-sale-equals-communication-and-streaming-from-unlawful-sources-is-illegal-c-52715-filmspeler/ (last accessed 1 August 2020)

Kuerbis, B., Mehta, I., & Mueller, M. (2017). *In Search of Amoral Registrars: Content Regulation and Domain Name Policy*. Atlanta: Internet Governance Project, Georgia Institute of Technology. Available at https://www.internetgovernance.org/wp-content/uploads/AmoralReg-PAPER-final.pdf (last accessed 1 August 2020).

Mahler, T. (2019). *Generic Top-Level Domains; A Study of Transnational Private Regulation*. Cheltenham: Edward Elgar.

Nordemann, J.B. (2020). *The functioning of the Internal Market for Digital Services: responsibilities and duties of care of providers of Digital Services*, Study Requested by the European Parliament's committee on Internal Market and Consumer Protection (IMCO)

Radu, R., & Hausding, M. (2020). Consolidation in the DNS resolver market – how much, how fast, how dangerous?, *Journal of Cyber Policy*, 5:1, 46-64, DOI: 10.1080/23738871.2020.1722191

Riordan, J. (2016). *The Liability of Internet Intermediaries*. Oxford University Press.

Radosavljev, P. (2017). For whom the copyright scale tips: has the CJEU established a proper balance of rights with its GS media case judgement?. *European Journal of Law and Technology*, *8*(3).

Rosati, E. (2017). GS Media and its implications for the construction of the right of communication to the public within EU copyright architecture. *Common Market Law Review*, *54*(4).

Rosati, E. (2016). "Hyperlinks and communication to the public: early thoughts on the GS Media decision", available at http://ipkitten.blogspot.com/2016/09/hyperlinks-and-communication-to-public.html (last accessed 1 August 2020).

Rosati, E. (2018). "Has the CJEU quietly changed the conditions for safe harbour availability?", available at http://ipkitten.blogspot.com/2018/08/has-cjeu-quietly-changed-conditions-for.html (last accessed 1 August 2020).

Schwemer, S. F. (2020). The regulation of abusive activity and content: a study of registries' terms of service. *Internet Policy Review*, *9*(1). DOI: 10.14763/2020.1.1448

Schwemer, S.F. & Schovsbo, J. H. (2020). What Is Left of User Rights: Algorithmic Copyright Enforcement and Free Speech in the Light of the Article 17 Regime. In: P. Torremans

(Ed.), *Intellectual Property Law and Human Rights* (4th edition, pp. 569-589). Alphen aan den Rijn: Wolters Kluwer.

Schwemer, S.F. (2019). Trusted notifiers and the privatization of online enforcement, *Computer Law & Security Review*, 35(6), 105339. DOI: 10.1016/j.clsr.2019.105339.

Schwemer, S. F. (2018). On domain registries and unlawful website content: Shifts in intermediaries' role in light of unlawful content or just another brick in the wall?. *International Journal of Law and Information Technology*, *26*(4), 273-293.

Truyens, M., & Van Eecke, P. (2016). Liability of domain name registries: Don't shoot the messenger. *Computer Law & Security Review*, *32*(2), 327-344.

Wang, Z., Huang, J., & Rose, S. (2018). Evolution and challenges of DNS-based CDNs. *Digital Communications and Networks*, *4*(4), 235-243.

van der Donk, B. B. (2020). How dynamic is a dynamic injunction? An analysis of the characteristics and the permissible scope of dynamic injunctions under European Law after CJEU C-18/18 (Glawischnig-Piesczek). *Journal of Intellectual Property Law & Practice,* jpaa071.

Case law

Judgment of 7 December 2006, *SGAE*, C-306/05, EU:C:2006:764
Judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54
Order of 19 February 2009, *LSG*, C-557/07, EU:C:2009:107
Judgment of 23 March 2010, *Google France and Google*, C-236/08 to C-238/08, EU:C:2010:159
Opinion of AG Jääskinen, delivered on 9 December 2010, *L'Oréal v eBay*, C-324/09, EU:C:2010:757
Judgment of 12 July 2011, *L'Oréal and Others*, C-324/09, EU:C:2011:474
Judgment of 4 October 2011, *Football Association Premier League and Others,* C-403/08 and C-429/08, EU:C:2011:631
Judgment of 19 April 2012, *Bonner Audio*, C-461/10, EU:C:2012:219
Judgment of 13 February 2014, *Svensson*, C-466/12, EU:C:2014:76
Judgment of 11 September 2014, *Papasavvas*, C-291/13, EU:C:2014:2209
Order of 21 October 2014, *BestWater*, C-348/13, EU:C:2014:2315
Opinion of AG Wathelet, delivered on 7 April 2016, *GS Media*, C-160/15, EU:C:2016:221
Judgment of 8 September 2016, *GS Media*, C-160/15, EU:C:2016:644
Judgment of 15 September 2016, *McFadden*, C-484/14, EU:C:2016:689
Judgment of 26 April 2017, *Filmspeler,* C-527/15, EU:C:2017:300
Judgment of 20 December 2017, *Uber Spain*, C-434/15, EU:C:2017:981
Judgment of 7 August 2018, *SNB-REACT*, C-521/17, EU:C:2018:639
Judgment of 18 October 2018, *Bastei Lübbe*, C-149/17, EU:C:2018:841
Judgment of 19 December 2019, *Airbnb Ireland*, C-390/18, EU:C:2019:1112
Judgment of 9 July 2020, *Constantin Film,* C-264/19, EU:C:2020:542

Opinion of AG Saugmandsgaard Øe, delivered on 16 July 2020, *Youtube and Cyando,* C-682/18 and C-683/18, EU:C:2020:586

Tallinna Ringkonnakohus (date of decision: 26.11.2018, entry into force: 15.01.2019, local case no: 2-14-6942)
Mediaset (RTI) v. Cloudflare, (order of Rome Court of First Instance of 13 March 2019, 1932/2019)
Mediaset (RTI) v. Cloudflare (order of Court of Rome VI of 24 June 2019, 26942/2019)
Universal Music GmbH (Germany), Cologne District Court (Landgericht Köln) on December 5, 2019, case no. 14 O 171/19