The Role of the Domain Name System and Its Operators in Online Copyright Enforcement

BRIP Working Papers No. 2

September 2022

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

THE ROLE OF THE DOMAIN NAME SYSTEM AND ITS OPERATORS IN ONLINE COPYRIGHT ENFORCEMENT

Prepared by Mr. Dean S. Marks, Attorney-at-law and Emeritus Executive Director and Legal Counsel, Coalition for Online Accountability, Los Angeles, United States of America, and Dr. Jan Bernd Nordemann, Attorney-at-law, Nordemann Czychowski & Partner, Berlin, and Honorary Professor, Humboldt University of Berlin, Germany[1]

STUDY COMMISSIONED BY THE BUILDING RESPECT FOR IP DIVISION

GLOBAL CHALLENGES AND PARTNERSHIPS SECTOR

WORLD INTELLECTUAL PROPERTY ORGANIZATION

Geneva, 2022

[1] This study was undertaken with the aid of funds provided by the Ministry of Culture, Sports and Tourism of the Republic of Korea (MCST). The views expressed in this document are those of the authors and not necessarily those of the Secretariat or of the Member States of WIPO.

TABLE OF CONTENTS

THE ROLE OF THE DOMAIN NAME SYSTEM AND ITS OPERATORS IN ONLINE COPYRIGHT ENFORCEMENT

Study prepared by Mr. Dean S. Marks and Dr. Jan Bernd Nordemann[2]

EXECUTIVE SUMMARY

Introduction

1. The domain name system (DNS) associates numerical Internet addresses with alphabetical names that are readily recognizable. It is a hierarchical, distributed and decentralized system that is extensible. The main DNS service providers that are the focus of this study are registries, registrars and DNS resolvers.

2. There is no single international treaty, organization or legal regime that regulates the DNS. The Internet Corporation for Assigned Names and Numbers (ICANN) governs generic top-level domains (gTLDs), and individual governments are responsible for policies and regulation of their particular country code top-level domains (ccTLDs).

DNS Providers and the Prevention of Copyright Infringements

3. Article 8 of the WIPO Copyright Treaty provides authors and copyright owners the right to prevent third parties from making their works available online without their authorization. National governments that are contracting parties to the WIPO Copyright Treaty have taken a variety of approaches in implementing this making available right.

4. Typically, users navigate to a website engaged in online copyright infringements by entering the domain name of the website in their browser or clicking on the domain name in search results. Because they enable Internet users to locate and access online sources of infringing content, DNS service providers, in particular registries, registrars and DNS resolvers, play a functional role in online copyright infringement.

5. Different approaches exist across jurisdictions with respect to the potential liability of domain name service providers for the unauthorized making available of copyright works by websites operating under domain names that these service providers, under contract, assign or administer. In general, however, the case law is not well developed and those courts that have considered the issue take the view that knowledge of the infringing activity and/or possibly some sort of bad faith is necessary to trigger the liability of domain name service providers. Courts in several jurisdictions have ordered that domain names be suspended and/or transferred pursuant to criminal seizure orders.

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

6. In contrast, in several jurisdictions case law exists with respect to the application of no-fault injunctive relief against domain name service providers to require them to disable or block resolution of domain names under which copyright-infringing websites operate. In considering any no-fault duty for DNS service providers, the principle of proportionality should evidently be applicable. It is necessary to find an adequate balance among the fundamental right to property (copyright holder), fundamental right to conduct a business (DNS service provider) and the right to access information (Internet user).

7. Remedies against DNS service providers have in particular met the proportionality test in cases of domain names that are used for websites which follow a copyright-infringing business model, systematically generating copyright infringements (so-called structurally copyright infringing websites). Under no-fault injunctive relief, for example, registries and registrars have been ordered to suspend or disable (disconnect) such websites' domain names, and registrars have been obliged also to freeze them (the registrar must not participate in transferring the domain to another registrar). DNS resolver providers have been ordered by courts not to resolve the respective domain name of such websites.

Contractual Position of DNS Service Providers

8. Domain name service providers, both for gTLDs and ccTLDs, operate under contractual arrangements. For gTLDs, both registries and registrars must enter into accreditation agreements with ICANN. Whether for gTLDS or ccTLDs, these contractual arrangements usually contain provisions that obligate registrants of domain names (i.e., the domain name holders) to refrain from using the domain names in conjunction with illegal activity, including copyright infringement. Under these contractual arrangements, domain name service providers have the authority to suspend or disable and freeze domain names under which websites engaged in pervasive copyright infringement operate. Despite having the contractual authority to suspend or disable such domain names, most domain name service providers will not do so upon notification by copyright owners. Instead, they will require either a court order or instruction from a government authority.

9. Suspending, disabling or blocking resolution of domain names is the only reactive measure domain name service providers can undertake with respect to websites and online services engaged in copyright infringement. However, domain name service providers can implement preventative measures to limit the misuse of domain names for websites engaged in illegal activity of all kinds, including copyright infringement. Such preventative, pro-active measures include, among others: (i) verifying the accuracy of the identity and contact information supplied by registrants and refusing to register domain names where such information is not accurate and (ii) implementing post-registration checks and reviews for the continued accuracy of identity and contact information and suspending domain names of registrants that do not correct inaccurate information.

10. Domain name service providers can undertake voluntary measures in the form of trusted notifier/trusted flagger arrangements with organizations having expertise in identifying copyright copyright-infringing websites. Two leading gTLDs registries, Donuts and Radix, have entered into such trusted notifier/flagger arrangements to address websites engaged in pervasive copyright infringement of films, television programs and sound/music

recordings. These trusted notifier arrangements were put into place in 2016 and are still operational.

Conclusion

11. The role of domain name service providers in addressing online copyright infringement is still in a state of development in terms of legal obligations and remedies (both liability and no-fault based) and voluntary actions. With respect to combating online copyright infringement, domain name service providers are capable of undertaking both preventative measures, as well as reactive measures.

I. INTRODUCTION TO THE DOMAIN NAME SYSTEM (DNS) AND DNS SERVICE PROVIDERS

A. GENERAL INTRODUCTION

1. The domain name system (DNS) associates numerical Internet addresses and resources with alphabetical names that are easy for end users of the Internet to recognize, remember and input into their connected devices. As described by the Internet & Jurisdiction Policy Network, "[d]omain names ensure a user-friendly conversion between human-readable identification strings and the long numerical Internet Protocol (IP) addresses indicating the location of a particular server on the network"[3]. Thus, for example, typing wipo.int into a web browser directs a user to the home page of WIPO's website. As explained by the Internet Corporation for Assigned Names and Numbers (ICANN), "the DNS helps users find their way around the Internet"[4].

2. A hierarchical and distributed system, the DNS has been a functional component of the Internet since the mid-1980s. The DNS was described in a 1987 paper by the Internet Engineering Task Force as "intentionally extensible" and "a tree structure" where "each node and leaf on the tree corresponds to a resource set (which may be empty)"[5]. As explained by one researcher, "[t]he DNS differs significantly from the rest of the Internet's decentralized and distributed architecture: it must be operated on a centralized basis to ensure that every domain name is unique and that a website name will always lead to the same address, regardless of the geographical location of the user typing the name in his web browser"[6].

3. Domain names typically consist of words separated by dots, such as redcross.org. The words are technically referred to as labels and the labels to the far right are the highest in the hierarchy[7]. For example, in redcross.org, ".org" is the top-level domain and "redcross" is a subdomain that is part of or belongs to the .org top-level domain.

4. Top-level domains are the highest level in the hierarchy of the DNS. In general, top-level domains are divided into two categories: (i) generic top-level domains (gTLDs), and (ii) country code top-level domains (ccTLDs). gTLDs consist of three or more letters or characters. Currently there are over 1200 gTLDs[8]. Examples of popular gTLDs include .com, .net, .org and .info. ccTLDs consist of two letters and follow the ISO 3166-1 alpha-2 standard published by the International Organization for Standardization[9]. Thus, for example, .ch is the ccTLD for Switzerland and .us is the ccTLD for the United States of America and .cn for China. According to the Council of European National Top-Level Domain Registries (CENTR), there exist over 315 million registered domain names, 68% of which belong to gTLDs and 32% of which belong to ccTLDs[10].

---

3 "Domains & Jurisdiction Program: Operational Approaches" Internet & Jurisdiction Policy Network, April 2019 at page 7: https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf.

4 https://www.icann.org/en/icann-acronyms-and-terms.

5 Mockapetris, Paul (November 1987) "Domain Names – Concepts and Facilities" Internet Engineering Task Force RFC 1034 at pages 1 and 7: https://datatracker.ietf.org/doc/html/rfc1034.

6 Caroline Bricteux, "Regulating Online Content through the Internet Architecture: The Case of ICANN's new gTLDs" 7 (2016) JIPITEC 229, at page 230, available at https://www.jipitec.eu/issues/jipitec-7-3-2016/4512/bricteux_regulating_online_content_through_the_internet_architecture_jiptec_7_3_2016_229.pdf.

7 Ibid. at pages 7-11.

8 See: https://icannwiki.org/Generic_top-level_domain.

9 https://en.wikipedia.org/wiki/Country_code_top-level_domain.

10 See CENTRstats Global TLD Report 2021/2 at page 3 available at: https://www.centr.org/library/library/statistics-report.html.

B. POLICY MAKING FOR GTLDS AND CCTLDS

5. The Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization that has technical management responsibility over the DNS, including root server management functions that support both gTLDs and ccTLDs. ICANN also coordinates the development and implementation of policies concerning gTLDs and accredits both registry operators and registrars with respect to gTLDs[11].

6. In contrast, the policies for ccTLDs – such as who may register a domain name in a particular ccTLD and what activities are prohibited by a website using a domain name belonging to a ccTLD – are subject to the authority of the government of the relevant country represented by the particular ccTLD. As explained in a paper published by the Organisation for Economic Co-operation and Development (OECD), "whereas gTLDs … are governed by rules set up by ICANN, ccTLDs, for their part, are under national jurisdiction for the definition of their policies and legal responsibilities"[12].

7. The DNS is not governed by an international treaty. National and regional laws, ICANN policies, contractual obligations, private-public arrangements, voluntary measures and self-regulation all play a role in how the DNS operates and how DNS service providers address online illegal activities[13].

C. DNS SERVICE PROVIDERS

a) Registry Operators (Registries)

8. Each top-level domain is administered by an entity called a registry operator, usually referred to simply as a registry. The registry maintains the authoritative master database of all domain names registered in that particular top-level domain and technically operates the top-level domain. Further, the registry maintains all administrative data, ensures that each domain name in the top-level domain is unique, and operates the authoritative name servers of the top-level domain. This allows servers across the Internet to translate domain names into IP addresses, which thus enable devices to connect to one another and for the website or online resource associated with a particular domain name to be reached by users around the world[14].

9. gTLD registries are typically for-profit entities. For example, Verisign – a for-profit American company – is the registry for the .com and .net gTLDs. Some gTLD registries are not-for-profit entities. For example, Public Interest Registry – a not-for-profit American company – is the registry for the .org gTLD.

10. In contrast, ccTLD registries are typically agencies or ministries of the government of the country associated with the particular ccTLD. The registry for the .kr ccTLD for the Republic of Korea, for example, is the Korea Internet & Security Agency. Frequently governments will contract with a non-governmental entity to serve as the registry of their ccTLD as is the case with Germany, where the registry for the .de ccTLD is DENIC, which is a not-for-profit cooperative[15].

---

11 See ICANN Bylaws at: https://www.icann.org/resources/pages/governance/bylaws-en.

12 https://www.oecd.org/sti/ieconomy/37730629.pdf at page 4.

13 European Commission, "Study on Domain Name System (DNS) Abuse" January 2022 at pp. 100-01 available at https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1.

14 See: https://www.icann.org/en/icann-acronyms-and-terms.

15 https://www.denic.de/en/about-denic/.

11. Every top-level domain, whether a gTLD or ccTLD, has only one registry. However, a registry may own and administer several gTLDs. Donuts, for example, is a for-profit American company that is the registry operator for more than 200 different gTLDs[16].

b) Registrars

12. A registrar is an entity that manages the registration of individual domain names, sometimes referred to as subdomains, within a top-level domain. It licenses – normally for a fee – to an individual or organization the right to use a particular domain name for a period of time and manages the registration process for the particular domain name. The registrar verifies that the domain name sought to be licensed by an individual or organization is available and meets the requirements of the registry of the top-level domain. The registrar enters into a contract with and also collects information, including contact information, from the individual or entity (registrant) reserving the right to use the particular domain name[17]. This information is commonly referred to as WHOIS data and includes the name, physical address, email address and phone number of the individual or entity seeking the right to register and use the particular domain name.

13. Registrars must be accredited by and enter into an agreement with the registry in order to register domains in a particular top-level domain. In essence, the registry serves as the "wholesaler" and the registrar serves as the "retailer" of domain names to the public[18].

14. A top-level domain, whether gTLD or ccTLD, may have multiple registrars offering/licensing to the public domain names within that particular top-level domain. Such registrars may be established and operating in countries around the world outside the country in which the registry is established. For example, over 2,000 registrars around the world offer .com domain names and are accredited by Verisign, the registry of the .com gTLD[19]. Similarly, registrars frequently offer domain names to the public in more than one top-level domain and will often register domain names in both gTLDs and ccTLDs. GoDaddy, for example, serves as a registrar for more than 500 different top-level domain names, including both gTLDs and ccTLDs.

c) Domain Resellers

15. A reseller is an organization affiliated with or under contract with one or more registrars to sell domain names and sometimes other services offered by the registrar(s) such as web hosting or email mailboxes. Resellers are bound by their agreements with the registrars whose services they sell and are not accredited by ICANN with respect to gTLDs[20].

16 https://donuts.domains/what-we-do/top-level-domain-portfolio/.
17 https://www.icann.org/en/icann-acronyms-and-terms.
18 https://en.wikipedia.org/wiki/Domain_name_registrar.
19 https://www.verisign.com/en_US/domain-names/domain-registrar/index.xhtml.
20 https://www.icann.org/resources/pages/register-domain-name-2017-06-20-en.

d) Privacy/Proxy Service Providers

16. A privacy or proxy service provider is a service that supplies alternative, reliable contact information for the registration data (WHOIS data) for a particular domain name in place of the identification and contact information of the registrant, which is the entity or natural person that is the actual/beneficial owner of the right to use the particular domain name[21].

e) DNS Resolvers

17. A DNS resolver is responsible for initiating and sequencing the queries that ultimately lead to a full resolution of the resource sought, e.g., translation of a domain name into an IP address[22]. Services of a DNS resolver are normally provided by the Internet access provider used. An Internet user may also choose to use the DNS resolver of a third party.

d) Internet Access Providers (ISPs)

18. An Internet access provider provides services to end users to access the Internet. It is not in and of itself a DNS service provider. Only insofar as the Internet access provider also provides and operates services of a DNS resolver can an Internet access provider also be classified as a DNS service provider.

II. INTRODUCTION TO SCOPE OF PROTECTION OF COPYRIGHT IN THE ONLINE ENVIRONMENT

A. COMMUNICATION TO THE PUBLIC AND MAKING CONTENT AVAILABLE TO THE PUBLIC UNDER INTERNATIONAL COPYRIGHT LAW

a) Article 8 WIPO Copyright Treaty

19. Article 8 WIPO Copyright Treaty supplements the rights of authors under the Berne Convention, which do not adequately cover acts of exploitation on the Internet. Article 8 WIPO Copyright Treaty obliges the contracting states to provide authors the right to prevent third parties from making their works available to others on the Internet without their consent. It reads as follows:

> "Without prejudice to the provisions of Articles 11(1)(ii), 11bis(1)(i) and (ii), 11ter(1)(ii), 14(1)(ii) and 14bis(1) of the Berne Convention, authors of literary and artistic works shall enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them."

20. The right of making content available to the public was inserted in particular to cover the dissemination of protected works on Internet websites of any kind, e.g., on-demand downloads, peer-to-peer filesharing, on-demand streaming. The agreed statements

---

[21] Final Report on the Privacy & Proxy Services Accreditation Issues Policy Development Process, 7 December 2015 at p. 7 https://gnso.icann.org/sites/default/files/filefield_48305/ppsai-final-07dec15-en.pdf.

[22] https://www.icann.org/en/icann-acronyms-and-terms?nav-letter=r&page=2.

concerning Article 8 WIPO Copyright Treaty clarify that the mere provision of physical facilities for enabling or making a communication does not in itself amount to a making available of the content. Still, this does not mean that DNS service providers and other intermediaries can never be liable for violation of the making available right as set forth in Article 8 WIPO Copyright Treaty. Case law from WIPO Member States shows that if the provision of physical facilities is combined with other factors, then intermediaries may be found to have violated the making the available right. Examples of such other factors include intent and breach of obligation, as is illustrated in the case law from the European Union discussed below.

b) European Union: Article 3(1) Copyright Directive 2001/29

21. The European Union has implemented Article 8 WIPO Copyright Treaty by Article 3(1) EU Copyright Directive 2001/29 (also called "InfoSoc Directive")[23]. This Article fully harmonizes the right of communication to the public and thus also the right of making available for all EU Member States. It reads as follows:

> "Member States shall provide authors with the exclusive right to authorise or prohibit any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them."

22. Recital 23 EU Copyright Directive 2001/29 states that this right should be understood in a broad sense covering all communication to the public not present at the place where the communication originates. This broad understanding is reflected in the case law of the European Court of Justice (CJEU).

23. Relying on Article 3(1) EU Copyright Directive 2001/29, the CJEU has extended communication to the public to acts of intermediaries, which play an "indispensable role" for its users to make illegal content available and deliberately intervene into the communication to the public. This is in particular true for link providers who set up hyperlinks to content hosted beyond their websites[24], providers of hardware with links[25], BitTorrent platforms[26], video sharing platforms (in the case: YouTube) and share hosting platforms (cyber lockers)[27]. This will be analyzed in more detail below[28].

---

23 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.

24 CJEU of 8 September 2016, C-160/15 – GS Media/Sanoma; CJEU of 26 April 2017, C-527/15 – Brein/Wullems (Filmspeler).

25 CJEU of 26 April 2017, C-527/15 – Brein/Wullems (Filmspeler).

26 CJEU of 14 June 2017, C-610/15 - Ziggo /Brein, paras. 36, 37.

27 CJEU of 22 June 2021, joined cases C-682/18 and C-683/18 - Peterson/YouTube et al. and Elsevier/Cyando, para. 77.

28 See below paras 60-64.

c) Copyright Law of the United States

24. Although the United States implemented the WIPO Copyright Treaty with the passage of the Digital Millennium Copyright Act in 1998 (DMCA), it did not change the copyright statute to specifically implement the Article 8 making available right. Instead, both the U.S. Copyright Office and Congress concluded that the existing statutory rights of distribution, public display and public performance already encompassed and incorporated the making available right[29].

25. This, however, has led to inconsistent decisions in the federal courts as to whether the uploading alone of copyrighted works without authorization constitutes a violation of the copyright owner's rights. Some courts have held that evidence of receipt of the work by a third party is necessary to constitute an infringement[30]. Indeed one federal court stated in 2015, "While the WIPO Treaty does recognize a 'making available right,' the treaty is not self-executing and it lacks any binding legal authority separate from its implementation through the [U.S.] Copyright Act"[31]. The U.S. Copyright Office undertook a detailed study concerning the making available right and published a lengthy report in 2016 entitled "The Making Available Right in the United States." Following an examination of the relevant statutory provisions, case law, and academic treatises, the Copyright Office concluded that "construing the [U.S.] Copyright Act to include a making available right is, at the very minimum, a reasonable interpretation" and that amending the Copyright Act to enact a separate making available right or communication-to-the-public right was not warranted[32].

26. The question of liability on the part of producers of software that facilitate the unauthorized online file sharing of copyrighted works by third parties was addressed by the U.S. Supreme Court in 2005. The Court found that a supplier of software – even if capable of non-infringing uses – can be held secondarily liable for the infringements committed by the users of the software under the concept of inducement. The Court held, "One who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties"[33].

d) Copyright Law of the Republic of Korea

27. The Korean Copyright Act (Act No. 17592) has also implemented Article 8 WIPO Copyright Treaty. Article 2 Korean Copyright Act provides for the following definitions:

> "The term 'public transmission' means transmitting works, stage performances, phonograms, broadcasts or database (hereinafter referred to as 'works, etc.') by making such available to the public by wire or wireless means so that the public may receive them or have access to them."

Article 18 (Right of Public Transmission) provides the author of a copyrighted work with the exclusive right to transmit his or her work in public.

---

29 "The Making Available Right in the United States" a Report of the Register of Copyrights, February 2016 https://www.copyright.gov/docs/making_available/making-available-right.pdf.

30 Ibid at pages 22-24.

31 BMG v. Cox, 149 F. Supp 634 at 638 (E.D. VA 2015).

32 "The Making Available Right in the United States" a Report of the Register of Copyrights, February 2016 https://www.copyright.gov/docs/making_available/making-available-right.pdf.

33 MGM v. Grokster, 545 US 913 (2005).

e) Copyright Law of India

28. The Indian Copyright Act has also implemented Article 8 WIPO Copyright Treaty. Section 2(ff) defines communication to the public as follows:

> "'communication to the public' means making any work or performance available for being seen or heard or otherwise enjoyed by the public directly or by any means of display or diffusion other than by issuing physical copies of it, whether simultaneously or at places and times chosen individually, regardless of whether any member of the public actually sees, hears or otherwise enjoys the work or performance so made available"[34].

Section 14 provides for the exclusive rights of copyright owners with respect to their works and includes the right of communication to the public[35].

f) Liability for Online Copyright Infringement

29. Liability for copyright infringement, both in the online and offline contexts, does not depend on intention[36]. Furthermore, in general many national copyright laws have distinct buckets or categories of liability, often referred to as "direct" or "primary" liability as opposed to "indirect" or "secondary" liability[37]. In the context of online copyright infringement, for example, a person who uploads to the Internet a copyright work without authorization would be liable as a direct infringer, i.e. would face direct liability. This liability is to be distinguished from liability of mere contributors to the infringement, i.e. the indirect infringer, who may face indirect or secondary liability. For example, a person or entity that supplies software that enables de-centralized peer-to-peer file sharing and distribution of copyrighted works without authorization could be liable under US law for so-called secondary infringement, if for example, the person supplied the software with knowledge that it would be used primarily for infringement, obtained a financial benefit from the infringement, and/or promoted the use of the software to infringe copyright[38]. A platform like YouTube where users upload copyright-infringing content could face secondary liability as an indirect contributor by providing the necessary facilities to infringe[39].

30. Accordingly, in the case of online infringement of copyright, Internet intermediaries and infrastructure providers may be subject to liability for copyright infringement depending on their functions (e.g., the reproduction and/or making available of works by hosting providers). Because these intermediaries and providers are both readily identifiable and often in a position to take action to disrupt online copyright infringement, concerns were raised about potential exposure to copyright liability and damage awards that could interfere with the growth of the online environment. As set forth below, many countries thus enacted safe harbor protections for Internet intermediaries. The tension between the damage caused by the ease and global scale of online copyright infringement as against the fear of stifling digital and online innovation and expansion due to copyright liability risks continues to this day. As noted in a 2015 OECD Study,

---

34 https://copyright.gov.in/documents/copyrightrules1957.pdf.

35 Ibid.

36 Harms, LTC (4th edition 2018) "A Casebook on the Enforcement of Intellectual Property Rights" at page 83, available at: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_791_2018.pdf.

37 Ibid. at page 81.

38 See MGM v. Grokster, 545 US 913 (2005).

39 CJEU of 22 June 2021, joined cases C-682/18 and C-683/18 - Peterson/YouTube et al. and Elsevier/Cyando, para. 77.

> "technological progress also facilitates digital piracy, as users employ various web-based workarounds and applications to distribute and exchange large amounts of pirated digital products instantaneously around the world. Hence, a significant volume of digital piracy occurs via the Internet[40].

At the same time, as explained in a WIPO Study:

> "legislators recognize the important role that intermediaries play on the Internet … [and] are clearly concerned that an expansionistic reading of indirect liability will stifle businesses and crimp the innovation and creativity that has led to the rapid and successful development of the Internet"[41].

Such safe harbor provisions for Internet intermediaries and service providers are analyzed below.

B. SAFE HARBORS FOR INTERNET INTERMEDIARIES AND SERVICE PROVIDERS

31. There is no binding international framework on a worldwide level harmonizing liability privileges ("safe harbors") for copyright infringement and other illegal content for Internet intermediaries and service providers, including DNS service providers.

a) The European Union Approach

32. In the European Union, the E-Commerce Directive provides for safe harbors in Articles 12 to 14 E-Commerce Directive[42]. The provisions exempt certain Internet service providers from liability for damages in cases where they would be liable under the applicable civil, criminal or administrative law regime. It is important to note that these privileges do not address liability; rather they establish exemptions from monetary damages in cases where liability for infringement is established. Privileged Providers are hosting services, providers who transmit information in a communication network or open access to networks ("mere conduit") or those who temporarily cache information. Articles 12 to 14 E-Commerce Directive will be reenacted with slight modification in the forthcoming Digital Services Act[43].

33. Internet Access Providers ("mere conduits") are privileged by Article 12 E-Commerce Directive, while cache providers enjoy liability privileges pursuant Article 13 E-Commerce Directive and hosting providers pursuant Article 14 E-Commerce Directive. For registries, registrars and DNS resolver service providers the legal situation is more difficult because no specific privilege exists for the provision of DNS services. It should be noted that registrars often offer web hosting as an optional service additionally to their domain service. If they host the content of a website, they are privileged as hosting providers. For the pure provision of DNS services only, a privilege under Article 12 (access provider privilege) or Article 13 E-Commerce Directive (cache provider privilege) comes into consideration.

---

40 OECD "Enquiries into Intellectual Property's Economic Impact" (2015), Chapter 5 "Copyright in the Digital Era: Country Studies" page 230.

41 Seng, Daniel "Comparative Analysis of the National Approaches to the Liability of Internet Intermediaries" (Preliminary Version) WIPO 2010 at pages 5-6.

42 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-Commerce Directive).

43 See Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC - COM/2020/825 final. See common position, as set out in Council of the European Union, document no. 14124/20 + ADD 1-3, June 15 2022, available at https://data.consilium.europa.eu/doc/document/ST-9342-2022-INIT/x/pdf.

34. Article 12(1) E-Commerce Directive reads as follows:

> "Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:
>
> (i) does not initiate the transmission;
> (ii) does not select the receiver of the transmission; and
> (iii) does not select or modify the information contained in the transmission".

35. Article 13(1) E-Commerce Directive reads as follows:

> "Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:
>
> (i) the provider does not modify the information;
> (ii) the provider complies with conditions on access to the information;
> (iii) the provider complies with rules regarding the updating of the information, specified in a manner widely recognized and used by industry;
> (iv) the provider does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information; and
> (v) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement".

36. According to the CJEU case law and Recital 42 E-Commerce Directive, the privileges envisage neutral and passive providers. The activity of Internet service providers who want to benefit from the privilege must be of a "mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored"[44]. Otherwise, the intermediary will not enjoy the privilege. DNS service providers generally provide a technical and automated service without knowledge of specific content on the websites. A contractual relationship with the infringer does not in itself constitute an active role. Consequently, DNS providers could be considered neutral service providers in the sense of the E-Commerce Directive.

---

[44] See for example CJEU of 7 August 2018, C-521/17 para. 47 – SNB-REACT; CJEU of 15 September 2016 C-484/14 para. 62 – McFadden; CJEU of 23 March 2010, C-236/08 to C-238/08 para. 113 – Google France and Google.

37. Whether the privileges of Articles 12 and 13 of the E-Commerce Directive apply to DNS service providers like registries, registrars and resolvers has not yet been decided by the CJEU[45]. The concept of "intermediary" appears to be broad[46]. However, as yet only one case in the CJEU has concerned the liability privilege of a domain service provider with an IP address rental and registration service[47]. Unfortunately, the information on the business model provided by the court initiating the preliminary ruling procedure was so vague that the CJEU only concluded that the privileges *could* apply if the service could be seen as a mere conduit, caching or hosting service[48]. Recital 27 of the proposal for a Digital Services Act amending the E-Commerce Directive points in the same direction[49]. It mentions that service providers establishing and facilitating the underlying logical architecture and proper functioning of the Internet, including technical auxiliary functions, can benefit from the privileges, to the extent that their services qualify as mere conduit, caching or hosting. The Recital specifically refers to DNS services and top–level domain name registries as an example.

38. In the end, on the European level it remains an open question whether DNS service providers may benefit from the liability privileges of the E-Commerce Directive in case of copyright infringements.

39. Among EU countries, Germany in particular has developed relevant case law:

- Registrars: The German Federal Supreme Court (BGH) has ruled that registrars are not privileged service providers[50]. According to the BGH the registrar neither transmits information nor does it provide access to information, but merely carries out the administrative processing of the domain registration by providing the registry with the required data[51]. In particular, the registrar is not a "mere conduit" access provider within the meaning of Section 8 German Telemedia Act (TMG), which transposes Article 12 E-Commerce Directive. With a similar reasoning and additionally referring to the contractual relationship with the infringer, two Courts of Appeal already ruled before the BGH that a registrar is not privileged like an access provider[52]. Nevertheless, the issue was controversial before the BGH's decision. For example, one Court of Appeal assumed that registrars provide access to content within the meaning of the privilege[53].

45 See Schwemer, Location, Location, Location! Copyright Content Moderation at Non-Content Layers, p. 386 with further references in footnote 45, in Rosati, Routledge Handbook EU Copyright Law, 2021; Nordemann, The functioning of the Internal Market for Digital Services: responsibilities and duties of care of providers of Digital Services, study requested by the IMCO committee of the European Parliament, 2020, p. 33, available here: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2020)648802.

46 CJEU of 7 July 2016, C-494/15 – Tommy Hilfiger.

47 CJEU of 7 August 2018, C-521/17 para. 40 et seq. – SNB-REACT.

48 CJEU of 7 August 2018, C-521/17 para. 52 – SNB-REACT.

49 See footnote 40.

50 German Federal Supreme Court (BGH) of 15 October 2020, I ZR 13/19 paras. 16,17 – Störerhaftung des Registrars.

51 German Federal Supreme Court (BGH) of 15 October 2020, I ZR 13/19 para. 17 – Störerhaftung des Registrars.

52 Court of Appeal (OLG) Saarbrücken of 19 December 2018, 1 U 128/17; Court of Appeal (OLG) Hamburg of 4 November 1999, 3 U 274/98.

53 Court of Appeal (OVG) Münster of 26 January 2010, 13 B 760/09.

- Registries: The BGH has not yet ruled on whether the registries' activities are privileged. The previous BGH case law only dealt with cybersquatting (trademark infringement by the domain name itself) and not liability for content on the websites[54]. Such cybersquatting cases have the significant difference that the cybersquatting has a direct connection to the role of the registry, which is to register domain names. This is not the case for copyright infringement committed on the website associated with the domain name. Against this background, it will be more suitable to look at the BGH case law on registrars concerning copyright infringements on the website operating under the domain name for which the registrar contracted with the registrant/website operator. The wording of the BGH in the registrar case makes it seem possible that the registry falls under the privilege for mere conduits (Article 12 E-Commerce Directive)[55]. In contrast to registrars, the registry not only performs administrative tasks, but is also technically involved in the IP address query process by operating the name servers of the top-level domain. An Administrative Court in Germany ruled that the registry provides access to content by assigning domain names to IP addresses and is therefore privileged like an access provider[56]. However, the BGH might also conclude that the registry does not enjoy the privilege because it only makes a partial contribution to resolving the domain into an IP address and is not directly involved in retrieving content.

- DNS Resolvers: With reasoning similar to that of the BGH in the case of the registrar, a Court of Appeal in Germany rejected the privilege of the DNS resolver: According to the court, the privilege does not cover every service provider who contributes to the access of information in any way. The DNS resolver only forwards requests to the name servers and then the IP address of the website back to the user, but it neither transmits the content of the website nor does it provide access to it[57].

b) The United States Approach

40. Like European Union law, the U.S. Copyright Act provides in Section 512 a series of safe harbors from monetary damages for copyright infringement for certain online service providers[58]. As does the E-Commerce Directive, these safe harbors do not establish rules concerning liability for infringement; rather they set forth the requirements for qualifying for limited relief (e.g., no monetary damages and limited injunctive relief) in the event a qualifying service provider were to be found directly or secondarily liable for copyright infringement. The categories of service providers that can qualify for the safe harbors, if they meet certain requirements, comprise access providers/mere conduits, caching systems, sites and services that store or host content at the direction of third-party users, and information location providers/search engines.

54 German Federal Supreme Court (BGH) of 27 October 2011, I ZR 131/10 – regierung-oberfranken.de; German Federal Supreme Court (BGH) of 17 May 2001, I ZR 251/99 – ambiente.de.
55 German Federal Supreme Court (BGH) of 15 October 2020, I ZR 13/19 para. 17 – Störerhaftung des Registrars.
56 Administrative Court (VG) Düsseldorf of 29 November 2011, 27 K 458/10.
57 Court of Appeal (Oberlandesgericht) Cologne of 9 October 2020, 6 U 32/20 paras. 98, 99 – HERZ KRAFT WERKE.
58 See Section 512 of Title 17 of the United States Code (the Copyright Act).

41. The requirements to qualify for the safe harbors vary by category of service provider. They include: (i) implementation of policies to terminate subscribers/users of the service that are repeat infringers, (ii) accommodation of standard technical measures, (iii) response to specific notifications of infringing materials by removing or disabling access to such materials, and (iv) not receiving a financial benefit directly attributable to infringing activity.

42. It appears unlikely that domain name registries or registrars would qualify for the Section 512 safe harbors given the relatively specific categories of service providers set forth in Section 512. So far, there have been no court decisions on this question. However, in the trademark context there is a specific provision granting a safe harbor to domain name registries and registrars and other "domain name registration authorit[ies]" from monetary damages for registration or maintenance of a domain name for a third party. This safe harbor against liability for trademark infringement applies unless there is a "showing of bad faith intent to profit from such registration or maintenance of the domain name"[59].

c) The China Approach

43. In China, a special regulation at one time excluded any liability of the registries. According to the administrative order for domain names of the Ministry for Data Industry, which is no longer in force, the registry was not responsible for infringements of rights by domain holders. However, this provision was deleted[60]. The Regulations on Protection of the Right of Communication through Information Networks, 2006 provide for safe harbors for access and caching service providers similar to those applicable under the EU E-Commerce Directive[61]. It appears from a decision of the Beijing Intellectual Property Court on liability for trademark infringement that general rules of accessory liability will apply to a registrar in relation to the infringing use of a domain name. Hence, where there is an act of IP infringement which the domain name registrar facilitates through its services, and the registrar knew or should have known that that act was an infringement, it will be liable with the infringer[62].

d) The Republic of Korea Approach

44. Article 102 Korean Copyright Act (Act No. 17592) also provides for a limitation on liability of online service providers. Online service providers are defined in Art. 2(30). The term "online service provider" means either of the following persons:

- a person who transmits, designates a route of, or provides connections to the works, etc. selected by users to deliver such works, etc. without any modification of their content through the information and communications networks … between points designated by users or
- a person who provides services to allow users to access the information and communications networks or reproduce or interactively transmit the works, etc. through the information and communications networks, or who provides or operates facilities therefor.

---

59 Section 1114(2)(D)(iii) of Title 15 of the United States Code (the Trademark Act).

60 Maaz, in: Bettinger, Handbuch des Domainrechts, 2nd Edition 2017, CN 63.

61 Articles 20 and 21, Decree of the State Council of the People's Republic of China No.468, Regulations on Protection of the Right of Communication through Information Networks, adopted at the 135th Executive Meeting of the State Council on May 10, 2006, effective as of July 1, 2006.

62 Beijing Intellectual Property Court, "Durex" trademark case report, March 23, 2021, https://bjzcfy.chinacourt.gov.cn/article/detail/2021/03/id/5903871.shtml.

These broad definitions would seem at least to cover registries.

45. Under Article 102(1), an online service provider which acts as a mere conduit or temporarily caches copies in the course of transmission is not liable for copyright infringement, provided that:

- it has not initiated the transmission;
- it has not selected the works or the works' recipients;
- it has adopted and reasonably implemented a policy that provides for termination of the accounts of persons who repeatedly infringe copyright; and
- it accommodates and does not interfere with standard technical measures used by the holder of right that are designed to identify and protect works (and meet conditions specified by Presidential Decree).

C. NO-FAULT INJUNCTIONS AGAINST INTERNET INTERMEDIARIES TO ADDRESS ONLINE COPYRIGHT INFRINGEMENT

46. On a worldwide level, there exists no harmonized framework for no-fault injunctions against Internet intermediaries to mitigate online copyright infringements. But some jurisdictions have introduced such legal tools into their enforcement systems requiring intermediaries to help mitigate online copyright infringement because they are in a good position to stop or interfere with the infringing activity.

a) The European Union Approach

47. In the European Union, even if the liability privileges for Internet intermediaries apply and provide a safe harbor, according to Articles 12 (3), 13 (2) and 14 (3) E-Commerce Directive, only claims for damages are excluded, but not injunction and removal claims. Recital 45 E-Commerce Directive reads as follows:

> "The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it".

48. The CJEU has clarified that the E-Commerce Directive does not preclude ancillary claims to injunction claims such as reimbursement of costs of giving formal notice and court costs incurred by a party filing a claim or legal action seeking injunctive relief[63].

49. The availability of injunctive relief against intermediaries is required under Article 8(3) EU Copyright Directive 2001/29 for copyright infringements and Article 11, third sentence Enforcement Directive for infringement of other intellectual property rights. Article 8(3) EU Copyright Directive 2001/29 reads as follows:

> "Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right".

63 CJEU of 15 September 2016, C-484/14 para. 78. – McFadden/Sony Music.

50. Recital 59 EU Copyright Directive 2001/29 provides the rationale for making these injunctive remedies against intermediaries available to copyright right holders. The reason is that intermediaries are simply in many cases best placed to bring infringing activities to an end. Injunction claims may be raised under Article 8(3) EU Copyright Directive 2001/29 not on grounds of fault, but because intermediaries are in a good position to help[64].

51. As to these injunction claims, Article 15 E-Commerce Directive, which prohibits the imposition of general monitoring duties on privileged providers, must be noted, as it limits the scope of possible injunction claims. The prohibition of general monitoring duties before notification of a specific infringement helps to balance the fundamental rights at stake as between the Internet provider, its users and the right holders[65]. It is important to note that Article 15 E-Commerce Directive does not stand in the way of more specific monitoring duties regarding certain specific infringements: Member States are obliged to be in a position to require intermediaries to take preventive measures against similar infringements in the future[66]. This may even include filtering duties as long as they are limited to a specific infringement[67]. The scope of these specific monitoring duties depends on the type of provider and its business model.

52. There is a trend within the EU to establish self-regulatory systems combined with state overview in relation to DNS blocks by access providers[68]. Self-regulatory systems have been agreed by right holders and access providers in various EU countries, including Denmark[69], the Netherlands[70] and Germany[71]. There are in particular to two models. The Danish and the Dutch model requires a court order against one national access provider in a sample case, which is then followed without further court order by the other national access providers, which are part of the self-regulatory agreement[72]. The German system involves a first level check by a self-regulated decision body (comprised among others of former Federal Supreme Court judges) and a second level check by the German Federal Network Agency, in charge of guaranteeing net-neutrality[73].

64 Shapiro, Directive 2001/29/EC on Copyright in the Information Society, in: Copyright in the Information Society: A Guide to National Implementation of the European Directive 54; Nordemann, The functioning of the Internal Market for Digital Services: responsibilities and duties of care of providers of Digital Services, study requested by the IMCO committee of the European Parliament, 2020, p. 26, available here: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2020)648802.

65 CJEU of 14 April 2011, C-70/10, para. 69 et seq. – Scarlet/SABAM; CJEU of 16 February 2012, C-360/10, para. 39 et seq. – SABAM/Netlog; CJEU of 15 September 2016, C-484/14, para. 87 – McFadden/Sony Music.

66 CJEU of 14 April 2011, C-70/10 para. 31. – Scarlet/SABAM.

67 For details see CJEU of 3 October 2019, C-18/18 – Eva Glawischnig-Piesczek/Facebook Ireland Limited; Nordemann, The functioning of the Internal Market for Digital Services: responsibilities and duties of care of providers of Digital Services, study requested by the IMCO committee of the European Parliament, 2020, p. 42 et seq., available here: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2020)648802.

68 Nordemann, Website Blocking under EU Copyright Law, p. 374 et seqq., in Rosati, Routledge Handbook EU Copyright Law, 2021.

69 https://sharewithcare.dk/.

70 https://www.acm.nl/en/publications/agreement-among-internet-providers-and-copyright-holders-regarding-blocking-websites-illegal-content.

71 See www.cuii.info (in German only).

72 See for the Dutch system: https://www.acm.nl/en/publications/agreement-among-internet-providers-and-copyright-holders-regarding-blocking-websites-illegal-content.

73 See for the German system: www.cuii.info (in German only).

b) The Republic of Korea Approach

53. Article 103(1) Korean Copyright Act (Act. No. 17592) provides for a similar provision as in EU law:

> "Any person who claims that his or her copyright and other rights protected under the Korean Copyright Act are infringed due to the reproduction or interactive transmission of works, through the use of services by an online service provider, may demand the online service provider, by vindicating the said facts, to suspend the reproduction or interactive transmission of the works".

As per Article 2, the term "interactive transmission" means, among types of public transmission, to make works, etc. available for the public so that the members of the public may have access at the time and place of their own choice.

c) The United States Approach

54. The United States has no statutory equivalent to the "no fault" injunctive relief provision of Article 8(3) of the EU Copyright Directive 2001/29. While Section 512(j) provides for the possibility of copyright owners to secure specific limited injunctive relief against Internet service providers that qualify for the safe harbor protections, the copyright owner would still have to establish infringement – either direct liability or secondary liability – on the part of the service provider. As discussed further below, in the context of establishing liability for copyright infringement on the part of a website or other online service, it is possible for copyright owners to obtain court orders that require service providers to terminate services to the infringing website or service without having to prove any liability on the part of the service provider. But such orders can only be obtained in the context of a judgment of infringement issued against a particular website or service.

d) Other Jurisdictions

55. Other examples of no-fault injunction regimes include Australia, Singapore and India. In Australia, the addressee of a no-fault blocking order is a "carriage service provider"[74]. The complex definition of this concept set out in section 78 of the Telecommunications Act 1997 probably does not include a DNS service operator. In Singapore, on the other hand, the definition of relevant service providers comprises "a person who provides services relating to, or provides connections for, the transmission or routing of data"[75]. This broad definition would seem to extend to DNS service providers. In India, the High Court of New Delhi in 2019 ordered injunctive relief with respect to Internet access providers to block access to thirty websites engaged in copyright infringement. In its judgment, the High Court stated that with respect to digital piracy, "India, like other countries, will need to work with Internet intermediaries as the main solution"[76].

---

74 Section 115A, Copyright Act 1968.

75 Section 193A, as inserted by section 47, Copyright (Amendment) Act 2004.

76 UTV Software Communication Ltd vs 1337X.To and Ors (2019) paragraph 72. Judgment and opinion available at: https://indiankanoon.org/doc/47479491/.

III. DNS SERVICE PROVIDERS AND THE PREVENTION OF COPYRIGHT INFRINGEMENTS

56. Websites engaged in copyright infringement operate under domain names, either a gTLD or a ccTLD. One remedy to address the copyright-infringing activity is for the domain name of the website to be "suspended" and "frozen". When a domain name is suspended, practically speaking the entire website associated with that domain name, including all the content on the website, any sub-domains and associated emails, is disabled. Neither registries, registrars nor DNS resolvers are able to address or technically remove individual pieces of content or URLs on a website. Suspending a domain name means that when a user types in the domain name into her website browser, it will not resolve or bring the user to the website; essentially the website is no longer visible on the Internet. However, as a technical matter, unless the website has been taken down by its hosting provider, it still remains available through the website's IP address[77]. As explained by one researcher:

> "Domain name suspension … is a powerful tool to deny access to online content. The registry, which controls the authoritative record for resolving each SLD (second level domain name) within its TLD, has the technical capacity for either deleting the connection between the domain name and the associated IP address in the database, or for diverting a domain name to another IP address, such as one pointing to a law enforcement message. Domain name resolution can also be suspended by the registrar that assigned the domain name. In both cases an Internet user who would type the web address containing the suspended domain name in his web browser would not be able to find the requested website. The DNS would return a non-existent or different domain response. This technique is easy to implement as it is not necessary to locate and confiscate the server hosting the content. Indeed, the content itself is not taken down – it can still be accessed via the IP address but most Internet users would be unable to do so, because they would not know the (numerical) IP address of a specific website"[78].

57. Domain name suspension[79], while technically simple for a registry or registrar to undertake, has been referred to as a "blunt tool." The Internet & Jurisdiction Policy Network has opined that "[a]cting at the DNS level should only be considered when it can be reliably determined that a domain is used with a clear intent of significant abusive conduct"[80].

58. Freezing the domain name means that it cannot be transferred to another party and the registrant information cannot be modified either[81]. As set forth in more detail in Section III. B below, registries and registrars reserve for themselves the right to suspend domain names that they administer or have registered, including if the domain name registrant uses the domain to conduct abusive or illegal activity.

---

77 Internet & Jurisdiction Policy Network, "Toolkit DNS Level Action to Address Abuses" March 2021 at p. 5: https://www.internetjurisdiction.net/domains/toolkit.

78 Bricteux, Caroline (July 2016) "Regulating Online Content through the Internet Architecture: The Case of ICANN's new gTLDs" at page 243: https://www.jipitec.eu/issues/jipitec-7-3-2016/4512/bricteux_regulating_online_content_through_the_internet_architecture_jiptec_7_3_2016_229.pdf.

79 Note that courts, researchers and academics sometimes use the terms "suspend," "disable," and/or "disconnect" interchangeably when referring to the action undertaken by either a registry or a registrar to stop a domain name from resolving to the IP address of the associated website and therefore prevent the ordinary Internet user from reaching or accessing the website.

80 Ibid. at p. 4.

81 See e.g., https://www.sidn.nl/en/nl-domain-name/frozen-domain-name.

59. DNS resolvers may also help to address copyright infringement. DNS resolvers are responsible for a full resolution in particular of a domain name into an IP address. If the website with copyright-infringing content uses a domain name, the DNS resolver could refuse this resolution. "The domain name has a high relevance for the accessibility of the content because hardly any user would access the website directly via the IP address instead", as the German Federal Supreme Court (BGH) put it[82].

A. JUDICIAL ENFORCEMENT OF COPYRIGHT AND DNS SERVICE PROVIDERS

a) Liability of DNS Service Providers for Copyright Infringement

60. The term liability as used here includes direct or primary liability (primary liability) by the direct infringer on the one hand and as an indirect contributor to the infringement (secondary liability) on the other hand[83]. The term "liability" normally provides for full legal consequences such as injunction claims and damage claims. However, the terminology regarding secondary liability varies at national level. Even within the European Union, such national concepts for secondary liability have different labels such as joint tortfeasor, accessory liability or authorization[84]. Beyond such ordinary liability (e.g., for injunction and damages), some jurisdictions also offer no-fault injunctions against intermediaries as described above in Section II C. This is treated separately from liability in its own chapter below with respect to DNS service providers[85].

61. In the European Union, the CJEU has extended communication to the public to acts of indirect contribution which, according to the classical understanding, fall more within the scope of secondary liability. This is in particular true for intermediaries, which play an "indispensable role" for its users to make illegal content available. Such an indispensable role is defined quite broadly. The intermediary plays such an "indispensable role" if – in case the services were not provided and managed – it would be impossible or, at the very least, more complex freely to share that (copyright-infringing) content on the Internet[86]. According to the case law of the CJEU link setters[87], providers of hardware with links[88], BitTorrent platforms[89], video sharing platforms (in the case: YouTube) and file-hosting platforms (cyberlockers)[90] play such an "indispensable role", if they are used to provide access to copyright-infringing content.

62. But an "indispensable role" is not the only criterion that must be taken into account. It is also relevant if the intervention of such an operator is deliberate. In particular, if the

---

82 German Federal Supreme Court (BGH) of 15 October 2020, I ZR 13/19 para. 19 – Störerhaftung des Registrars.

83 See also para. 29.

84 See for a comparative analysis Dinwoodie, A Comparative Analysis of the Secondary Liability of Online Service Providers, in Dinwoodie (Editor), Secondary Liability of Internet Service Providers (2017) page 20 et seq.; see also Angelopoulos, Online Platforms and the Commission's New Proposal for a Directive on Copyright in the Digital Single Market, page 23 et seq. with a comparative analysis of national approaches in the UK, France and Germany.

85 See below paras 78 et seq.

86 CJEU of 22 June 2021, joined cases C-682/18 and C-683/18 - Peterson/YouTube et al. and Elsevier/Cyando; see in particular para. 77.

87 CJEU of 8 September 2016, C-160/15 – GS Media/Sanoma; CJEU of 26 April 2017, C-527/15 – Brein/Wullems (Filmspeler).

88 CJEU of 26 April 2017, C-527/15 – Brein/Wullems (Filmspeler).

89 CJEU of 14 June 2017, C-610/15 - Ziggo /Brein, paras. 36, 37.

90 CJEU of 22 June 2021, joined cases C-682/18 and C-683/18 - Peterson/YouTube et al. and Elsevier/Cyando, para. 77.

intermediary intervenes in full knowledge then this factor must be considered[91]. This leads to a concept which results in duties of care for the "indispensable role" intermediary. The linker is liable for linking to content, uploaded in breach of copyright by a third party, if the linker knew or ought to have known that the content linked to was illegal[92]. The seller of media players which knowingly contain links to copyright-infringing content by third parties also is liable for infringement of the making available right[93]. The same is true for knowingly indexing content to enable unlawful sharing via a peer-to-peer network by third parties[94]. The case law was recently applied also to platforms (hosting providers). The operator of a video sharing platform (in the case: *YouTube*) and the operator of a share hosting platform (cyber locker) make content available to the public if their users illegally upload protected works and the platform contributes, beyond merely supplying the platform, to giving access to such content to the public in breach of copyright. For such a contribution, it is necessary to meet one of the following (alternative) requirements:

- that operator has specific knowledge that protected content is available illegally on its platform and refrains from expeditiously deleting it or blocking access to it;
- that operator, despite the fact that it knows or ought to know, in a general sense, that users of its platform are making protected content available to the public illegally via its platform, refrains from putting in place the appropriate technological measures that can be expected from a reasonably diligent operator in its situation in order to counter credibly and effectively copyright infringements on that platform; or
- that operator participates in selecting protected content illegally communicated to the public, provides tools on its platform specifically intended for the illegal sharing of such content or knowingly promotes such sharing, which may be attested by the fact that that operator has adopted a financial model that encourages users of its platform illegally to communicate protected content to the public via that platform[95].

63. All these cases have in common that the intermediary only aids, encourages or intensifies a copyright infringement that is actually committed by third parties. Nevertheless, the intermediary itself is liable (secondary liability) in these cases as it breached a duty of care.

64. So far, this case law has not been applied to DNS service providers by the CJEU. But liability for DNS service providers appears possible in case they are used by third parties for copyright infringements. First, a DNS service provider needs to play a sufficiently "indispensable role" in making the content available as required by the CJEU.[96] It is sufficient for an intermediary that – if the services were not provided and managed – it would be impossible or, at the very least, more complex to freely share that (copyright-infringing)

91 CJEU of 22 June 2021, joined cases C-682/18 and C-683/18 - Peterson/YouTube et al. and Elsevier/Cyando; see in particular para. 78-82.

92 CJEU of 8 September 2016, C-160/15 – GS Media/Sanoma.

93 CJEU of 26 April 2017, C-527/15 – Brein/Wullems (Filmspeler).

94 CJEU of 14 June 2017, C-610/15 - Ziggo /Brein.

95 CJEU of 22 June 2021, joined cases C-682/18 and C-683/18 - Peterson/YouTube et al. and Elsevier/Cyando; see in particular para. 102.

96 CJEU of 22 June 2021, joined cases C-682/18 and C-683/18 para. 68 – Peterson/YouTube et al. and Elsevier/Cyando.

content on the Internet[97]. This could be said for registries and registrars. The domain name is highly relevant for the accessibility of the content because hardly any user would access the website directly via the IP address instead[98]. Also, services of registries and registrars are provided directly or indirectly to the infringer.

65. That said, there needs to be a deliberate intervention by the intermediary according to the CJEU, constituting a breach of a duty of care. The CJEU ruled that it was not proportionate to expect legal business models to check all content for infringements without a notification that narrows the monitoring duties to certain works[99]. It is supported by national trademark case law (e.g., from Austria, Belgium, France, Germany and Sweden) that DNS providers are not obligated to check domains and content for infringements prior to notification by the right holders or prior to court orders[100]. Thus, a liability may only be considered if the DNS service provider does not cease to provide its service to the infringing website after notification of the infringement.

i. Registries

66. A Swedish District Court and a Court of Appeal ruled that the registry, although it contributed with intent to the infringement when it decided not to take down the domains of an infringing BitTorrent website, is not secondarily for the copyright infringement occurring on the website. The reason is that the registry does not act for financial gains but in the public interest and because of its administrative function it is not obligated to check the legality of the website content. The examination of legality should be reserved to the courts and the registry should only act upon a court order[101]. The President of a Commercial Court in Belgium also ruled that the registry is not fully liable as a perpetrator or accessory[102].

67. In Italy, a court ruled that the registry could be liable for aiding and abetting trademark infringements by the domain name in exceptional cases where it is obvious that the applicant is not authorized to use the domain name[103]. However, this case related to the domain names themselves and not to infringing website content.

97 CJEU of 22 June 2021, joined cases C-682/18 and C-683/18 - Peterson/YouTube et al. and Elsevier/Cyando; see in particular para. 77.

98 German Federal Supreme Court (BGH) of 15 October 2020, I ZR 13/19 para. 19 – Störerhaftung des Registrars.

99 CJEU of 14 April 2011, C-70/10, paras. 47 et seq. – Scarlet/SABAM.

100 German Federal Supreme Court (BGH) of 15 October 2020, I ZR 13/19 para. 30 – Störerhaftung des Registrars; German Federal Supreme Court (BGH) of 17 May 2001, I ZR 251/99 – ambiente.de; District Court Stockholm of 19 May 2015, B 6463-13 and Svea Court of Appeal of 12 May 2016. B 5280-15; Commercial Court Brussels of 9 August 2013, 2012/12072/A; Court of Appeal Versailles of 15 September 2011, 09/07860 – Association AFNIC vs SAS Francelot; Court of Appeal Paris of 19.10.2012 – Air France et als v. AFNIC/EuroDNS; Austrian Federal Supreme Court (OGH) of 12.9.2001, 4 Ob 176/01p – fpo.at II.

101 Schwemer, On Domain Registries and Unlawful Website Content (March 10, 2018) International Journal of Law and Information Technology, Volume 26, Issue 4, 1 December 2018, Pages 273–293, DOI: 10.1093/ijlit/eay012, Available at SSRN: https://ssrn.com/abstract=3107547; Truyens/Van Eecke, Liability of domain name registries: Don't shoot the messenger, Computer Law & Security Review (2015), p. 6; with reference to District Court Stockholm of 19 May 2015, B 6463-13 and Svea Court of Appeal of 12 May 2016. B 5280-15.

102 Strowel/Daems, in: Bettinger, Handbuch des Domainrechts, 2nd Edition 2017, BE 103 referring to commercial court Brussels of 9.8.2013, 2012/12072/A, available at www.rdc-tbh.be.

103 Fabbio, in: Bettinger, Handbuch des Domainrechts, 2nd Edition 2017, IT 92 with reference to Trib. Napoli of 26.02.2002, Dir. Inf. 2002, 1005, 1038 ff.

ii. Registrars

68. In 2006 the Tribunal de Grande Instance de Paris ruled in a cybersquatting case that the registrar, even without notification, is guilty of aiding and abetting unlawful activities of the registrant and is therefore not only obliged to suspend the domain name but is also liable for damages[104]. However, this case related to cybersquatting and was therefore connected to the domain name itself, rather than activity conducted by a website operating under the domain name.

69. A District Court in Germany ruled that a registrar might be liable for damages as an accessory to copyright infringements on the website. However, the mere notification of the infringement is not sufficient to trigger such liability. Rather, the registrar must also have knowledge that the notification is accurate and the alleged infringement actually exists[105]. The same court stated that if the court orders a disconnection or suspension of the domain, the registrar must not participate in transferring the domain to another registrar. Otherwise, the registrar would be liable as an accessory (aider)[106]. This meant that the registrar had to "freeze" the domain. This judgment was confirmed by the Court of Appeal[107]. These rulings show that providing domain name registration services by a registrar to individuals or entities who operate a website engaged in copyright infringement is not in itself sufficient for liability where the registrar does not have clear knowledge of the infringing activity.

70. In China, until 2013, Internet service providers such as registrars, were jointly liable (in most cases contributory liability) with the perpetrator for damages if they failed to take action against the infringement despite having knowledge of the infringement or being notified with substantial evidence or in some cases just because they neglected their duty of care[108]. According to the current legal situation, the domain has to be disconnected only if the registrar knows or ought to have known that the content infringes copyrights, although according to the prevailing opinion, service providers are not subject to a general monitoring obligation[109]. In general, Chinese tort law specific liability rules provide that Internet services providers are jointly liable with the perpetrator for damages if the infringing content is not blocked upon knowledge of the infringement[110].

71. In the United States, the court cases addressing the potential direct or secondary liability of domain name registries and registrars for intellectual property infringement relate to trademark, and more specifically cybersquatting where the relevant domain name is alleged to infringe on the plaintiff's trademark rights. Because of the safe harbor provided by the Anti-cybersquatting Consumer Protection Act (ACPA), which is part of the Trademark Act, plaintiffs have generally failed to meet the burden of establishing that the registry or registrar had the "bad faith intent to profit from [the] registration or maintenance of the

104 Tribunal de Grande Instance, Paris of 10 April 2006 – Sté Rue du Commerce v. Sté Brainfire Group et Sté Moniker Online Service Inc.
105 District Court (Landgericht) Cologne of 5 December 2017, 14 O 125/16 para. 69 – The PirateBay.
106 District Court (Landgericht) Cologne of 5 December 2017, 14 O 125/16 para. 100.
107 Court of Appeal (Oberlandesgericht) Cologne of 31 August 2018, 6 U 4/18 – The PirateBay.
108 Maaz, in: Bettinger, Handbuch des Domainrechts, 2nd Edition 2017, CN 66; Wan, Internet Service Providers' Vicarious Liability Versus Regulation of Copyright Infringement in China, Journal of Law, Technology and Policy, Vol. 2011, No. 375, 2011, p. 382, available at SSRN: https://ssrn.com/abstract=1975702; for ISPs.
109 Maaz, in: Bettinger, Handbuch des Domainrechts, 2nd Edition 2017, CN 67; for no general monitoring duties of ISPs and their duty to act upon specific knowledge in China see Wang, Development of Hosting ISPs' Secondary Liability for Primary Copyright Infringement in China – As Compared to the US and German Routes. IIC 2015, 275, 278 f.
110 Maaz, in: Bettinger, Handbuch des Domainrechts, 2nd Edition 2017, CN 68.

domain name," which would be required to deprive the registry or registrar from the safe harbor protections[111].

72. Given (i) the closer nexus of allegations of cybersquatting to the services provided by domain name registries and registrars and (ii) the high bar set by the ACPA for liability on the part of registries and registrars for cybersquatting, it is unsurprising that no case law in the United States exists addressing either primary or secondary liability on the part of registries or registrars for copyright infringement based on the infringing activity of a website operating under a domain name that has been licensed by a registrar and/or administered by a registry.

iii. DNS Resolvers

73. There seem to be no cases where operators of DNS resolvers were found to be liable for third party copyright infringements committed on the website for which they resolve the domain. Such cases are usually dealt with under the regimes of no-fault injunctions (see below[112]).

iv. Conclusion

74. For primary or secondary liability, the legal comparison shows that the mere registration of and administration of domain names is not sufficient to establish fault or strict liability on the part of registries, registrars or DNS resolvers for the copyright-infringing content on the website.

75. In most countries, DNS service providers are not primarily liable. The perpetrator is the website operator or domain owner and is primarily liability as the direct copyright infringer.

76. Nevertheless, secondary liability of DNS service providers for infringing content is possible. It is more likely that the registrars will be found liable on a secondary basis than will the registries. This is due to the fact that registries perform more administrative functions and act to a certain extent in the public interest; whereas registrars have a closer relationship with domain holders/registrants through their contracts. In any case, simply registering or administering the domain name is not sufficient to establish secondary liability. Rather, further elements must be added that constitute fault in order to justify secondary liability. In most cases, this involves knowledge of the infringement or that the service provider ought to have known that the content infringes copyrights if it had exercised due diligence. At this point it is crucial whether a DNS service provider "ought to have known" before it has been informed about copyright-infringing content on the website connected to the domain name. In other words, the question arises if a duty of the DNS service provider is recognized to check the content of a website before it has been put on notice about copyright infringements. In some countries, even knowledge of an infringement is not sufficient to establish a form of secondary liability; rather, a court order must declare the content infringing before liability can be considered.

111 See, e.g Berhad v. GoDaddy, 897 F. Supp. 2d 856 (N.D. Cal. 2012); Lockheed Martin v. Network Solutions, 141 F. Supp. 2d 648 (N.D. Tex. 2001).

112 See paras 78 et seq.

77. In summary, there is no consistent case law regarding the requirements to establish primary or secondary liability of DNS service providers on an international level with respect to websites engaged in copyright infringement.

b) No-fault Injunctions Against DNS Service Providers

78. As mentioned above[113], in the European Union the availability of injunctive relief against intermediaries is mandatory under Article 8(3) EU Copyright Directive 2001/29 for copyright infringements and under Article 11, third sentence Enforcement Directive for infringement of other intellectual property rights. The concrete implementation of these Directives is in the hands of the EU member states. Hence, national practice in the European Union differs to a certain extent.

79. For instance, the mandatory injunctive relief against intermediaries under Article 8(3) EU Copyright Directive 2001/29 is in German law provided by the concept of *Störerhaftung* (interferers' responsibility). In the event of an infringement, a claim for injunctive relief may be asserted against anyone who – without being a perpetrator or participant – in any way intentionally contributes to the infringement of the protected right. The giving of support to the action of a third party may also suffice as a contribution, provided that the person against whom the claim is asserted had the opportunity to prevent the infringement. In order not to unduly extend liability to third parties who have not themselves carried out the unlawful act, the injunctive relief requires the violation of reasonable obligations of conduct[114]. These obligations of conduct differ regarding the type of provider at stake and may also include duties to prevent similar infringements in the future.

i. Registries

80. Based on the national implementation of Article 8(3) EU Copyright Directive 2001/29 and Article 11, third sentence Enforcement Directive there is case law of the Member States of the European Union confirming that injunctive relief against registries may be sought even if they provide a technically neutral service. Although the prerequisites for injunctive relief vary from one EU Member State to another, the hurdles are generally quite high.

81. Most cases against registries are cybersquatting (trademark) cases regarding claims concerning the domain names themselves. Regarding trademark infringing domain names, a French Court of Appeal emphasizes that a registry must only block or suspend a domain upon a court order instructing the registry to do so[115]. According to the trademark case law of the German and the Austrian Federal Supreme Courts (BGH and OGH), there is injunctive relief against the registry for the top-level domain only if it is informed of an obvious infringement, which can be easily recognized[116]. The reason for limiting the injunctive relief is (like in the Swedish judgements[117] mentioned above) that the registry acts

---

113 See II C(a) above, and in particular the wording of Article 8(3) EU Copyright Directive 2001/29 and its legal background.

114 German Federal Supreme Court (BGH) of 17 August 2011, I ZR 57/09 – Stiftparfüm.

115 Truyens/Van Eecke, Liability of domain name registries: Don't shoot the messenger, Computer Law & Security Review (2015), p. 6 with reference to Court of Appeal Versailles of 15 September 2011, 09/07860 – Association AFNIC vs/ SAS Francelot, unpublished.

116 German Federal Supreme Court (BGH) of 27 October 2011, I ZR 131/10 – regierung-oberfranken.de; German Federal Supreme Court (BGH) of 17 May 2001, I ZR 251/99 – ambiente.de; Austrian Federal Supreme Court (OGH) of 13.9.2000, 4 Ob 176/01p – fpo.at I; Austrian Federal Supreme Court (OGH) of 12.9.2001, 4 Ob 176/01p – fpo.at II.

117 See para. 66.

without the intention of making profit and performs its task in the interest of all Internet users[118]. According to the courts, stricter concepts would jeopardize the quick and inexpensive registration of domains.

82. However, copyright infringement cases in general do not relate to infringing domain names, but to the content accessible via the domain name. In Belgium, the Anti-Piracy Federation (BAF) brought a case against the registry because of copyright-infringing content on the websites under a .be domain. In its ruling, the court held that the registry even after being notified of infringing content does not have to disconnect the domain name. Rather, the registry has to act only if an infringement is determined by a court ruling[119].

83. Nevertheless, the Belgian case[120] shows that registries may face injunctive relief requiring them to block access to infringing content by disabling a domain solely due to their position as intermediaries, without any fault on their part. This is in accordance with the requirements of Article 8(3) EU Copyright Directive 2001/29. Also noteworthy is the fact that the court ruled that right holders are not required to take action against third parties like other online service providers or the infringer before contacting the registry.

ii. Registrars

84. In Germany, the so-called *Störerhaftung*[121] implements the EU law concept of no-fault injunctions into German law (Article 8(3) EU Copyright Directive 2001/29 and Article 11, third sentence Enforcement Directive). *Störerhaftung* requires an adequate causal contribution to the infringement and that it is proportionate to act or refrain from contributing. Accordingly, the registration of a domain is sufficient to require the registrar to take action against infringing content and to disconnect the domain[122]. However, according to the case law of the German Federal Supreme Court ("BGH") the registrar is not required to act until the right holders have complied with certain rules and procedures: the registrar is obliged to disable the domain name under the same conditions as the access provider is obliged to block a website[123]. This is to protect justified rights of the DNS service providers and of the Internet users affected by the disconnection. As with access providers, the registrar must (1) be notified of a clear infringement and (2) is only obliged to take action if the content on the website is predominantly infringing[124]. Otherwise, a disconnection of the domain name would be disproportionate regarding the fundamental right of Internet users to access information. This will usually mean that action against registrars for disconnection of a domain name used for copyright infringements will require a website which follows a

118 German Federal Supreme Court (BGH) of 17 May 2001, I ZR 251/99 – ambiente.de. It should be noted that in these cases the registries were non-profit organizations responsible for administering a ccTLD. However, with respect to the vast majority of gTLDs and even some ccTLDs, their respective registries are commercial, for-profit entities.

119 Commercial Court Brussels of 9 August 2013, No. 2012/12072/A. See also the report about the decision by Schwemer, On Domain Registries and Unlawful Website Content (March 10, 2018) International Journal of Law and Information Technology, Volume 26, Issue 4, 1 December 2018, Pages 273–293, p. 10, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3107547.

120 Commercial Court Brussels of 9 August 2013, No. 2012/12072/A.

121 Literal translation: Responsibility of the disturber.

122 German Federal Supreme Court (BGH) of 15 October 2020, I ZR 13/19 para. 19 – Störerhaftung des Registrars.

123 See leading EU case on website blocking: CJEU C-314/12 of 27 March 2014 – UPC Telekabel; overview on further case law by Nordemann, Website Blocking under EU Copyright Law, p. 357 et seqq., in Rosati, Routledge Handbook EU Copyright Law, 2021.

124 German Federal Supreme Court (BGH) of 15 October 2020, I ZR 13/19 paras. 30, 33 – Störerhaftung des Registrars; German Federal Supreme Court (BGH) of 26 November 2015, I ZR 174/14 paras.26 et seq. – Störerhaftung des Access-Providers.

copyright-infringing business model, systematically generating copyright infringements (so-called structurally copyright-infringing websites)[125]. In addition, both providers can only be successfully sued for injunctive relief after the right holders have unsuccessfully taken action against the operator of the website and the hosting provider, unless such action lacks any reasonable prospect of success (so-called subsidiarity requirement)[126]. This subsidiarity requirement, however, has been critiqued not to be in line with EU law[127]. For injunctive relief against access providers, also courts in other EU member states have explicitly refused to apply a subsidiarity requirement[128]. Right holders must already demonstrate in the notification of infringement that the conditions for a claim exist[129]. The reason why the registrar is subject to stricter obligations than the registry is that the registrar acts with the intention of making a profit and does not act solely in the public interest as the registry does[130].

85. Before the decision of the German Supreme Court, the German Court of Appeal Cologne had applied less strict standards for action against registrars. According to this court, right holders do not have to take action against third parties before making claims against registrars[131].

86. In accordance with the German case law, the District Court of Luxembourg stated that the registrar provides its customers with access to the Internet and is therefore to be classified as an intermediary within the meaning of Article 8(3) EU Copyright Directive 2001/29[132]. As a consequence, right holders can apply for injunctions against registrars. However, the District Court of Luxembourg set lower hurdles for claims against registrars than the German Federal Supreme Court when it ordered the registrar EuroDNS to cease providing services with regard to six infringing domains. Like the German Court of Appeal Cologne, the District Court of Luxembourg ruled that there is no subsidiarity requirement since the law does not require a right holder to act first against the actual infringers before applying for injunctive relief against an intermediary. Regarding non-infringing content on the websites, the court points out that some non-infringing content does not preclude a suspension of the domain and that this content can be accessed through other channels. One must take into account that the websites in dispute systematically and massively infringed copyrights through streaming.

87. Two cases from Ukraine show what court orders against registrars can look like in interim relief[133]. In both cases the defendants used the domains to infringe trademarks of the plaintiff. But not only did the domain name itself violate the trademark rights of the plaintiff. The defendants also offered goods and services on the website that infringed

125 More details on structurally copyright-infringing websites: Nordemann, Website Blocking under EU Copyright Law, p. 358, in Rosati, Routledge Handbook EU Copyright Law, 2021.
126 German Federal Supreme Court (BGH) of 15 October 2020, I ZR 13/19 para. 31 – Störerhaftung des Registrars; German Federal Supreme Court (BGH) of 26 November 2015, I ZR 174/14 para. 83 – Störerhaftung des Access-Providers.
127 Nordemann, Website Blocking under EU Copyright Law, p. 357 (372-373), in Rosati, Routledge Handbook EU Copyright Law, 2021.
128 Austrian Oberster Gerichtshof (Austrian Supreme Court) of 24 October 2017, 4 Ob 121/17y; Tribunal de Grande Instance de Paris, FNDF v. Google and others, of 15 December 2017, 17/13471.
129 German Federal Supreme Court (BGH) of 15 October 2020, I ZR 13/19 para. 40 – Störerhaftung des Registrars.
130 German Federal Supreme Court (BGH) of 15 October 2020, I ZR 13/19 para. 30 – Störerhaftung des Registrars.
131 Court of Appeal (Oberlandesgericht) Cologne of 31 August 2018, 6 U 4/18 para. 75.
132 District Court of Luxembourg of 22 February 2017, case no. 52/2017.
133 Court order of 17 June 2016, case no. 753/9682/15; Court order of 11 November 2019, case no. 757/19365/19.

trademark rights. The courts ordered interim measures against the registrars of the domains in dispute. In the first case the court ordered the registrar only to set the status of the domains to “clientHold”, which results in the domain no longer resolving to the website's IP address, and to suspend the delegation and support of the domains[134]. In the second case the court ordered measures which can be summarized as a complete “Freezing” of the domains: Additional to the obligation to set the “clientHold” status the court prohibited the registrars from changing, deleting or transferring the domain[135].

88. In France, claims against registrars require compliance with higher formal requirements. A Court of Appeal has applied the principles developed for registries' liability to registrars[136]. Because of the strictly technical nature of the service, the Court held that registrars are not obliged to monitor domain names for infringements. They are not even required to act upon a notification of an infringement. Rather, like registries, registrars are only obliged to suspend or disable a domain upon a court order instructing them to do so. In another registrar case the parties agreed that the registrar would switch the DNS servers of the domain in dispute to fictional DNS servers in order to block access to the website; would stop the legal, administrative and technical management of the said domain name by its current holder by means of the attribution of the "Clienthold" and "clienttransferprohibited" status; and would not renew the domain[137]. The registrar did not oppose because it was not even doubted that registrars fall under the provision implementing Article 8(3) EU Copyright Directive 2001/29 and are therefore subject to no-fault injunctions.

89. Although the United States does not have a statutory provision equivalent to Article 8(3) of the EU Copyright Directive 2001/29, injunctive relief against registries and registrars (and other intermediaries such as hosting providers and payment processors) can be obtained without a showing of fault on the part of the registry or registrar in the context of an infringement action against the website or service directly engaged in the IP infringement. The source of these injunctions is Federal Rule of Civil Procedure 65(d) concerning the contents and scope of injunction and restraining orders, which provides as follows:

> “(1) *Contents.* Every order granting an injunction and every restraining order must:
>
> (A) state the reasons why it issued;
> (B) state its terms specifically; and
> (C) describe in reasonable detail – and not by referring to the complaint or other document – the act or acts restrained or required.
>
> (2) *Persons Bound.* The order binds only the following who receive actual notice of it by personal service or otherwise:
>
> (A) the parties;
> (B) the parties’ officers, agents, servants, employees, and attorneys; and

134 Court order of 17 June 2016, case no. 753/9682/15.
135 Court order of 11 November 2019, case no. 757/19365/19.
136 Court of Appeal Paris of 19 October 2012, Air France et al. versus Afnic, EuroDNS; see also Murphy, The Role of a Domain Name Registrar as an Internet Intermediary, p. 6 and https://www.lavoix.eu/en/news/91/april-2013-air-france-versus-afnic-eurodns.
137 Tribunal de Grande Instance de Lille of 23 November 2017, 17/08143.

(C) other persons who are in active concert or participation with anyone described in Rule 65(d)(2)(A) or (B)".

90. Under the leading case in this area concerning registrars and registries, the Court, after finding that the defendant websites were engaged in illegal trademark infringement and counterfeiting, found that even though the registry of the domain names of the infringing websites was not a party or defendant in the lawsuit, it could still be subject to an injunction to suspend/disable the domain names "to enjoin it from aiding and abetting, or participating in defendants' unlawful activities" under Federal Rule of Civil Procedure 65(d)[138].

91. U.S. federal courts have routinely relied on Federal Rule of Civil Procedure 65(d) to enjoin a broad range of non-party Internet intermediaries and service providers, including domain name registrars and registries, hosting providers, payment processors, search engines, online advertising agencies, content delivery networks, reverse proxy services and others from continuing to provide their services to websites that have been found to infringe intellectual property rights, including trademark, copyright and prohibitions on the circumvention of technical protection measures. Where these providers have argued that they are merely "passive" providers of automated services and therefore not in "active concert or participation" with the infringing websites, the courts have rejected these arguments and imposed injunctions to require these non-party providers to cease providing services to the infringing websites[139].

92. In other countries outside of the European Union and the United States, it appears that no-fault injunctive relief against intermediaries, including DNS service providers, is possible. In Russia, for example, no-fault injunctive relief against information intermediaries is possible. The cases involve primarily hosting providers, user generated content ("UGC") websites, and cyberlockers. Regarding registrars and registries, the courts have not yet taken a clear position. In one case however, the court ordered a preliminary injunction against a registrar of a website with copyright-infringing content to disable connecting the domain[140].

iii. DNS Resolvers

93. The case law of the European Union has seen the first cases where copyright holders were granted injunctive relief against DNS resolvers for third party copyright infringements committed on the website for which they resolve the domain. Such cases are usually dealt with under the EU regime of no-fault injunctions pursuant Article 8(3) EU Copyright Directive 2001/29[141].

138 *The North Face Apparel Corp. v. Fujian Sharing Imp. & Exp. Ltd. Co., No. 10* CIV. 1630 (AKH), 2011 WL 12908845 (S.D.N.Y. June 24, 2011).

139 See e.g., Artista Records, LLC v. Tkach, 122 F. Supp 3d 32 (S.D.N.Y. 2015); Showtime Networks, Inc. v. Doe 1, Temporary Restraining Order and Order to Show Cause, No. 15-CV-3147 (CD Cal. April 30, 2015); Warner Bros. Ent., Inc., v. Doe, Preliminary Injunction Order, No. 14-CV-3492 (SDNY May 29, 2014); AACS-LA v. Shen, Order, No. 14-CV-1112 (SDNY Mar. 4, 2014).

140 Tuschino District Court of 19 June 2015, case no. 1121/15.

141 See above II C(a).

94. Two German courts have applied the requirements for DNS blocks of access providers[142] also to DNS blocks by DNS resolver operators[143]. There also seems – generally speaking – to be no reason to distinguish between an access provider (also) providing DNS resolver services to its users and a DNS resolver provider which does not also provide access services. Accordingly, the DNS resolver is not required to act until the right holders have complied with the requirements developed for access providers under EU law:

- Website blocks on the basis of Article 8 (3) EU Copyright Directive 2001/29 may lead to conflicts with fundamental rights protected under EU law. Right holders may rely on the protection of copyright and related rights (Article 17 (2) EU Charter of Fundamental Rights). Furthermore, the right of freedom to conduct a business may be affected on the side of the provider (Article 16 EU Charter of Fundamental Rights). Furthermore, the Internet user's right to freedom of information may become relevant when content on the Internet is blocked (Article 11 EU Charter of Fundamental Rights). In the leading EU law decision *UPC Telekabel,* the CJEU assessed the conflict between these applicable fundamental rights under EU law for website blocks[144].
- As a first outcome in website blocking cases, the CJEU seems to be of the opinion that the cost of blocking measures must be borne by the providers. This may be proportionate even if the blocking measures represent significant costs for the provider[145]. Accordingly, access providers must expect to have to install website blocks and should therefore be expected to have the corresponding technical infrastructure in place. Costs for setting up relevant technical equipment for the first time should therefore not be relevant to assess proportionality[146].
- Another issue of proportionality when balancing the different fundamental rights may be overblocking. Overblocking comes into consideration when a blocking measure blocks more content then required to bring an end to the specific copyright infringement. The CJEU held in UPC-Telekabel that the measures implemented by the provider must be strictly targeted, in the sense that they are sufficiently effective in bringing the rights infringement to an end but not to impair the Internet users in their freedom to access information lawfully[147]. DNS blocks – implemented by access providers, but also by DNS resolvers – may lead to overblocking, in case the targeted website also contains legal information. According to the case law of the German Federal Supreme Court (BGH) a qualitative assessment must be applied. Legal

142 See leading EU case: CJEU C-314/12 of 27 March 2014 – UPC Telekabel; overview on further case law by Frosio/Bulayenko, EUIPO Study on Dynamic Blocking Injunctions, 2021, p. 14 et seq., available here: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Dynamic_Blocking_Injuctions/2021_Study_on_Dynamic_Blocking_Injuctions_in_the_European_Union_FullR_en.pdf Nordemann, Website Blocking under EU Copyright Law, p. 357 et seqq., in Rosati, Routledge Handbook EU Copyright Law, 2021.

143 Court of Appeal (Oberlandesgericht) Cologne of 9 November 2020, 6 U 32/20 para. 93; District Court Hamburg of 12 May 2021, 310 O 99/21.

144 CJEU C-314/12 of March 27, 2014 paras 49 et seq. - *UPC Telekabel*; see also Nordemann, Website Blocking under EU Copyright law, page 357 (367), in Rosati, Routledge Handbrock EU Copyright law 2021. Frosio/Bulayenko, EUIPO Study on Dynamic Blocking Injunctions, 2021, p. 22 et seq.

145 CJEU C-314/12 of March 27, 2015 para. 50 – *UPC-Telekabel.* The Supreme Court of the United Kingdom, however, held in Cartier International AG & Ors v British Telecommunications Plc & Anor [2018] UKSC 28 (13 June 2018) that the providers' costs of compliance with a blocking order should be borne by the right holder claimants.

146 District Court Munich I, February 1, 2018, 7 O 17.752/17, para. 69 at seqq.; Nordemann *op cit* page 372.

147 CJEU C-314/12 of March 27, 2015 para. 56 – *UPC-Telekabel.*

content must not play a sufficient role on the targeted website ("fallen nicht ins Gewicht"). It is also important to note that the BGH from the start excluded any illegal content (even if infringing rights of third parties) from the assessment. The BGH also held that the blocking of websites with 4% legal content would be proportionate in any case.[148]

- The requirement to keep DNS blocks proportionate and thus to avoid disproportionate overblocking will usually mean that action against registrars for disconnection of domain name used for copyright infringements will require a website which follows a copyright-infringing business model, systematically generating copyright infringements (so-called structurally copyright-infringing websites)[149].
- In addition, under German law DNS resolver providers can only be sued for injunctive relief after the right holders have unsuccessfully taken action against the operator of the website and the hosting provider, unless such action lacks any reasonable prospect of success (so-called subsidiarity requirement)[150]. This subsidiarity requirement, however, has been critiqued not to be in line with EU law[151]. For injunctive relief against access providers, also courts in other EU member states have explicitly refused to apply a subsidiarity requirement[152].

95. Right holders must already demonstrate in the notification of infringement that the conditions for a claim exist[153].

96. In many cases, the operators of websites blocked by DNS blocks try to circumvent the blocks by communicating to the website's users new alternative domain names, which have not yet been blocked. This may render administrative or judicial DNS blocking orders, which are limited to certain domain names, ineffective. Consequently, so-called dynamic blocking orders are granted in various countries. In its Guidance on the IP Rights Enforcement Directive (IPRED), the European Commission has favored such dynamic injunctions which are drafted so as to permit the right holder to give notice to the respondent ISP to extend the scope of the order to cover a new URL without the need for a fresh judicial procedure[154].

97. There may be one difference, however, regarding proportionality between DNS blocks by access providers on the one hand and DNS blocks by DNS resolver operators on the other hand. While access providers operate their DNS servers usually only within the territorial scope of their (national) access offer, DNS resolver operators may provide services

148 BGH of November 26, 2015 I ZR 174/14 para. 55 et seqq. - *Stoererhaftung des Accsess Providers.*

149 More details on structurally copyright-infringing websites: Nordemann, Website Blocking under EU Copyright Law, p. 358, in Rosati, Routledge Handbook EU Copyright Law, 2021.

150 German Federal Supreme Court (BGH) of 15 October 2020, I ZR 13/19 para. 31 – Störerhaftung des Registrars; German Federal Supreme Court (BGH) of 26 November 2015, I ZR 174/14 para. 83 – Störerhaftung des Access-Providers.

151 Nordemann, Website Blocking under EU Copyright Law, p. 357 (372-373), in Rosati, Routledge Handbook EU Copyright Law, 2021.

152 Austrian Oberster Gerichtshof (Austrian Supreme Court) of 24 October 2017, 4 Ob 121/17y; Tribunal de Grande Instance des Paris, FNDF v. Google and others, of 15 December 2017, 17/13471.

153 For notifications to registrars: German Federal Supreme Court (BGH) of 15 October 2020, I ZR 13/19 para. 40 – Störerhaftung des Registrars.

154 European Commission, Communication to the European Parliament, the Council and the European Economic and Social Committee, Guidance on certain aspects of Directive 2004/48/EC, COM (2017) 708 final, page 21; Frosio/Bulayenko, EUIPO Study on Dynamic Blocking Injunctions, 2021, page 16 et seq., with extensive examples for case law from the various EU member states.

across borders. Copyright protection is provided territory by territory as a bundle of national rights. Usually, a national court will only be competent to issue DNS blocking orders for websites for the territory of the national copyright law infringed. Courts may – generally speaking – not order DNS resolver operators to DNS block websites outside the territory of their jurisdiction. That said, DNS resolver operators are in a position to technically implement DNS blocks ordered only for certain territories by identifying the territory, where the DNS resolver users are located. This puts DNS resolver providers in a position to choose whether they want to implement the DNS block for all jurisdictions of their service or only within the jurisdiction for which the DNS blocking order has been issued.

98. In India, the High Court of New Delhi undertook a comprehensive survey of website blocking case law around the world in a 2019 decision[155]. That case involved 30 websites that had been determined via an *ex parte* lawsuit to be engaged in copyright infringement. The case included a request by the plaintiffs to require Internet access providers in India to block access to the infringing websites and for government agencies to supervise the implementation of such website blocks. The Court acknowledged that the plaintiffs were not asserting any fault or active involvement of the access providers in committing the infringements, but rather that these entities were pleaded into the case "for the purpose of evolving an effective and balanced relief"[156].

99. The Court gave a high-level description of website blocking case law that has been established and stated that "at least forty-five countries have either adopted and implemented, or are legally obligated to adopt and implement, measures to ensure that ISPs take steps to disable access to copyright infringing websites"[157]. Among the non-EU countries the Court identifies are Australia, Brazil, Indonesia, Israel, Malaysia, Republic of Korea, Russia, Singapore, Turkey and the United Kingdom. In determining that it has the authority to order website blocking, the Court stated that it "is of the opinion that it has ample powers to mould the relief to ensure that plaintiffs' rights are adequately protected"[158].

100. The Court undertook an analysis of the arguments posed by some groups that the Internet should largely be left free of restrictions and determined that "supporting website blocking for sites dedicated to piracy does not make one an opponent of a free and open internet" and that "advocating limits on accessing illegal content does not violate open Internet principles"[159].

101. The Court also engaged in a detailed analysis of what types of websites constitute rogue websites or flagrantly infringing online locations (FIOL) and held that the website need not host the infringing content in order to qualify as a rogue website/FIOL. Furthermore, the Court rejected a test or standard that such a website should only contain or facilitate access to illicit or infringing material. Rather the Court adopted a qualitative test (as opposed to a quantitative test) examining such factors as whether the primary purpose of the website is to

155 UTV Software Communication Ltd vs 1337X.To and Ors (2019) Judgment and opinion available at: https://indiankanoon.org/doc/47479491/.
156 Ibid. at paragraph 5.
157 Ibid. at paragraph 87.
158 Ibid. at paragraph 29.
159 Ibid. at paragraph 55.

commit or facilitate copyright infringement, the flagrancy of the infringement, a disregard for copyright generally, etc.[160].

102. Finally, in deciding what type of website blocking should be ordered, the Court determined that blocking on a URL-by-URL basis for specific pieces or instances of infringement would not be effective, proportionate nor practical. Instead, the Court adopted domain name blocking and quoted from a prior lower court decision that "if a domain name itself is blocked, to continue with the infringing activity becomes a cumbersome, time consuming and money spending exercise"[161]. Furthermore, recognizing that pirate websites will often seek to circumvent website blocking injunctions by acquiring new domain names to operate under, the Court issued a dynamic order that allows the plaintiffs to identify new or additional domain names to be blocked under the order "in the event they merely provide new means of accessing the same primary infringing websites that have been injuncted"[162].

iv. Conclusion

103. In the European Union, no-fault injunctive relief against registrars and registries and DNS resolvers is possible according to case law because of the national laws transposing Article 8(3) EU Copyright Directive 2001/29 and Article 11, third sentence Enforcement Directive. Every act contributing to an infringement is sufficient for injunctive relief. Also, DNS service providers seem to be in a good position to help fight the copyright infringements on the website, as DNS services (in particular by registries and registrars) are important to facilitate the infringement.

104. For registrars, most courts agree that they can be sued for no-fault injunctive relief and must suspend (disconnect) domain names. However, there are quite significant differences as to when this duty exists. Some courts impose the restriction that not too much lawful content may be affected by the suspension of the domain name. Some courts also apply the so-called subsidiarity requirement that the right holders must first take action against third parties (the website operator, the domain owner, other intermediaries such as hosting providers), although for website blocking cases involving access/mere conduit providers this requirement does not represent the prevailing view in the EU Member States. There are also differences in the point in time at which registrars have to take action: already after the infringement has been reported or only after a court order. It should be borne in mind that in case the registrar has a duty to disconnect/suspend, the registrar must also not participate in transferring the domain to another registrar or registrant, i.e., must "freeze" the domain name; otherwise, the registrar could even be (fault) liable as an accessory (aider)[163].

105. For registries, case law regarding copyright-infringing content on websites is scarce. Most cases relate to trademark infringing domains. Obtaining no-fault injunctive relief orders against registries appears to be subject to at least the same requirements that have been developed for registrars. Some courts – such as the German courts – even argue for stricter requirements (than for registrars) due the registries' responsibility to provide an efficient domain name system.

106. In countries outside the European Union the legal situation is less clear as to whether the registries and registrars, like other intermediaries, have to help to combat copyright infringements. For example, in Taiwan Province of China, the Intellectual Property Court dismissed a claim against a registrar, finding that the registrar bore no responsibility for

160 Ibid. at paragraph 59.
161 Ibid. at paragraph 63.
162 Ibid. at paragraph 107.
163 See above para. 69; German District Court (Landgericht) Cologne of 5 December 2017, 14 O 125/16 para. 100; see also above Ukrainian Court order of 11 November 2019, case no. 757/19365/19.

verifying the domains and the contents therein, and that the claimant should bring a legal claim directly against the alleged counterfeit operation holding the domain despite the fact that the WHOIS information provided to the registrar by the registrant was false. The Court held that, notwithstanding the claim of false domain registrant information, the registrar's responsibility stops with taking the domain information, and that the registrar is not responsible for verifying the domain registration information[164].

107. However, in the United States no-fault injunctive relief against registrars and registries is possible and has been regularly obtained in federal lawsuits involving claims of trademark and copyright infringement against websites engaged the infringing activity. This occurs where courts have found such infringement – based on a temporary restraining order, preliminary injunction or final judgment – and then enjoined non-party registrars and registries from continuing to provide services to such infringing websites.

108. DNS blocks by access providers and blocks by DNS resolver operators are technically comparable to those directed at registries or registrars and should pose parallel legal questions, in particular regarding proportionality. It seems to be the common view that DNS blocks by DNS resolvers should only be permitted with respect to websites predominantly consisting of copyright infringements, because in these cases disproportionate over-blocking will not be an issue. This will usually mean that successful legal action will require a website that follows a copyright-infringing business model, systematically generating copyright infringements (so-called structurally copyright-infringing websites)[165]. Website blocking via DNS blocks has been embraced by EU member states and several countries around the world outside of the EU.

c) Criminal Seizure Orders

109. Civil law is not the only instrument to achieve the disabling of domain names under which copyright-infringing content can be found. Especially if the domain name is notorious for a systematically infringing business model, seizure of the domain name under criminal law is also an option. In the USA and Canada[166], domain name seizure has become a relevant tactic in law enforcement. In the United States, for example, thousands of domain names have been seized by the federal government via criminal orders under a program called "Operation in our Sites" that is overseen the National Intellectual Property Rights Coordination Center[167]. Criminal seizure orders have also been used in Europe to permanently disable and prevent the use of certain domain names.

110. For example, in 2009 the Italian Supreme Court of Cassation confirmed that, at the request of the prosecutor, the infamous BitTorrent website "The Pirate Bay" could be the object of preventive seizure under Article 321, Penal Procedure Code, effectively requiring ISPs to block access to it[168]. A Swedish court ordered the seizure of the domain name of the

164 Intellectual Property Court Ruling 2015 Min-Chen-Zhi-No.3; available at: https://law.judicial.gov.tw/FJUD/data.aspx?ty=JD&id=IPCV,104%2c%e6%b0%91%e6%9a%ab%2c3%2c20150226%2c1.

165 See above para. 84.

166 For the trend of domain seizures in the US and Canada: https://www.ifrahlaw.com/crime-in-the-suites/domain-name-seizure-its-not-just-a-u-s-law-enforcement-tactic/.

167 See: https://www.iprcenter.gov/file-repository/ipu-operation-in-our-sites-2016.docx/view. Under Title 18 United States Code §2323, property used or intended to be used to commit or facilitate specific copyright offences is subject to forfeiture to the U.S. Government.

168 Supreme Court of Cassation, Cass. pen, Sez. III, Sent. 49437/09 29 September 2009.

same website from the owner because of illegal activities[169]. The District Court held that a domain name should be considered a form of intellectual property and can therefore, under the provisions of the Copyright Act, be seized. The court found that the registry's actions in this case, on the other hand, were permitted. Therefore, there were no grounds to allow the prosecutor's motion for forfeiture regarding the registry.

111. Sweden's Supreme Court later confirmed that the right to a domain name constitutes property which may be confiscated.[170] The decision is based on the fact that domain names are traded and a domain name can have a substantial financial value. Also, the European Court of Human Rights has stated that the right to a domain name constitutes a right to property which is protected by Article 1 of Protocol I to the European Convention for the Protection of Human Rights and Fundamental Freedoms.[171] According to this decision, the term 'property' in accordance with the aforementioned article is not limited to physical property. In the case of assets that are not physical, it is crucial that the ownership gives rise to certain financial rights and thus has a financial value. Given that domain names can give rise to advertising revenues and be sold, exclusive rights to a domain name have a financial value and therefore constitute property in the sense of the provision.

112. The decision is backed up by the Supreme Court of Norway, which also found that domain names may be confiscated[172]. The case concerned the question of seizure of the right to use the domain name "popcorn-time.no", a BitTorrent website which was used to make movies and TV-shows illegally available to the public. The court found that the seizure would stop the contribution of illegal content and thus was necessary with respect to an effective enforcement of the penal provision. The seizure was considered proportionate with reference to the fact that the consequences for the domain name holder were considered to be minimal while on the other hand a large amount of copyright-infringing content was made available. Freedom of speech did not call for a different conclusion.

113. In Denmark domains that have been used for copyright-infringing activities can be seized in an ex parte proceeding against the Danish domain registry. Courts have ruled that under section 804(1) of the Danish Administration of Justice Act, a third party who is not a suspect in the case, can be ordered on the application of the police to hand over an object which could serve as evidence in cases of public/government prosecution[173].

B. CONTRACTUAL OBLIGATIONS OF DNS SERVICE PROVIDERS WITH RESPECT TO COPYRIGHT INFRINGEMENT

114. Separate and apart from court ordered relief against DNS service providers – whether on the basis of liability, no-fault injunctive orders, or criminal seizure orders – DNS service providers operate under contracts that often address the issue of use of domain names to carry out illegal activities, including copyright infringement.

169 District Court Stockholm of 19 May 2015, B 6463-13; M. Truyens, P. Van Eecke, Liability of domain name registries: Don't shoot the messenger, Computer Law & Security Review: The International Journal of Technology Law and Practice (2015) p. 6.

170 Supreme Court of Sweden of 22 December 2017, case no. B 2787-16.

171 See European Court of Human Rights of 18 September 2007 – Paeffgen GmbH v. Germany, dec. nos. 25379/04, 21688/05, 21722/05 and 21770/05, p. 9.

172 Supreme Court of Norway of 17 September 2018, HR-2019-1743-A (case no. 19-057105STR-HRET).

173 https://edri.org/our-work/ex-parte-domain-name-seizures-denmark/.

a) gTLDs and ICANN Accreditation Agreements

115. In the gTLD space, every registry and every registrar must enter into an accreditation agreement with ICANN. The agreement for registries is called the Registry Agreement ("RA") and the agreement for registrars is called the Registrar Accreditation Agreement ("RAA"). The current versions of both the RA and the RAA have provisions that address the misuse of a website operating under a domain name registered under the relevant gTLD to commit abusive or illegal conduct, including copyright infringement.

116. With respect to the RA, the relevant provision reads:

> "[R]egistries shall include a provision in the Registry-Registrar Agreement that requires registrars to include in their Registration Agreements a provision prohibiting registrants from distributing malware, abusively operating botnets, phishing, piracy, trademark or **copyright infringement**, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name" (emphasis added) [174].

117. With respect to the RAA, the relevant provision reads:

> "Registrar shall maintain an abuse contact to receive reports of abuse involving Registered Names sponsored by Registrar, including reports of Illegal Activity. Registrar shall publish an email address to receive such reports on the home page of Registrar's website (or in another standardized place that may be designated by ICANN from time to time). Registrar shall take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse"[175].

118. "Illegal Activity" is defined in the RAA as "conduct involving use of a Registered Name sponsored by Registrar that is prohibited by applicable law and/or exploitation of Registrar's domain name resolution or registration services in furtherance of conduct involving the use of a Registered Name sponsored by Registrar that is prohibited by applicable law"[176].

119. Note that the language concerning a Registered Name sponsored by Registrar means a particular domain name that a registrar has licensed and registered for use by a particular registrant, which may be a natural or legal person.

b) ccTLDs and National Policies

120. With respect to ccTLDs, it is up to each individual country to determine its own contractual provisions concerning the registry-registrar agreements and any obligations concerning provisions that a registrar must include in its registration agreement with individual registrants for a particular domain name in the ccTLD. For example, for the .eu

---

174 ICANN 2017 Registry Agreement, Specification 11 paragraph 3(a) https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf.

175 ICANN 2013 Registrar Accreditation Agreement, section 3.18 https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#raa.

176 Ibid. at section 1.13.

ccTLD the agreement between EURid, the registry operator for the .eu ccTLD, and a registrar states:

> "You will ensure and document that each Registrant for whom you register a Domain Name has accepted the Rules in effect at the time the Registration is made and complies with all requirements set forth in the Rules, including but not limited to the confirmation by the Registrant that, to their knowledge, the request for Domain Name Registration is made in good faith and does not infringe the rights of any third party; and that the Registrant meets the eligibility criteria as defined in the Rules"[177].

121. One of the terms and conditions set forth in the Rules applicable to all registrants of an .eu domain name provides:

> "the Registrant has the following obligations: […]
>
> To use the Domain Name in such a way that **does not violate any third-party rights**, applicable laws, or regulations, including discrimination on the basis of race, language, sex, religion, or political view;
>
> Not to use the Domain Name (i) in bad faith or (ii) for any unlawful purpose" (emphasis added)[178].

122. For the .us ccTLD, there is an Acceptable Use Policy that applies to all registrants of .us domain names. One provision of the Policy states:

> By registering a name in the usTLD, you represent and warrant that you will not use that registration for any illegal purposes, including without limitation, to:
>
> a. distribute malware or engage in malicious hacking, bot-netting, phishing, pharming, fast flux hosting, fraudulent or deceptive practices;
> b. use, promote, encourage the promotion of, or distribute child abuse images or engage in the exploitation of minors in any way;
> c. sell or distribute pharmaceuticals;
> d. infringe the intellectual property rights of any other person or entity including, without limitation, counterfeiting piracy or trademark or copyright infringement;
> e. impersonate any person or entity, or submit of information on behalf of any other person or entity, without their express prior written consent;
> f. violate the privacy or publicity rights of any other person or entity;
> g. promote or engage in any spam or other unsolicited bulk email;
> h. distribute software viruses or any other computer code, files or programs designed to interrupt, destroy, or limit the functionality of any computer software, hardware, or telecommunications equipment or computer or network hacking or cracking;

177 EURid Registrar Agreement, Version 8 19-10-2019, Paragraph 4.1 https://eurid.eu/d/7583416/Registrar_agreement_en.pdf.

178 EURid Terms and Conditions, Section 3, https://eurid.eu/en/other-infomation/document-repository/.

i. interfere with the operation of the usTLD or services offered by the usTLD; or

j. otherwise engage in activity that is contrary to U.S. law or usTLD Policies"[179] (emphasis added).

123. For the .cn ccTLD, Article 27 of China's Internet Domain Name Regulations provides as follows:

> "Any of the following contents shall not be included in any domain name registered and used by any organization or individual:
>
> those that are against the basic principles prescribed in the Constitution;
>
> those jeopardize national security, leak state secrets, intend to overturn the government, or disrupt of state integrity;
>
> those harm national honor and national interests;
>
> those instigate hostility or discrimination between different nationalities, or disrupt the national solidarity;
>
> those violate the state religion policies or propagate cult and feudal superstition;
>
> those spread rumors, disturb public order or disrupt social stability;
>
> those spread pornography, obscenity, gambling, violence, homicide, terror or instigate crimes;
>
> those insult, libel against others and infringe other people's legal rights and interests; or
>
> other contents prohibited in laws, rules and administrative regulations" (emphasis added)[180].

124. Many registrars include in their terms of service provisions that prohibit domain name registrants (whether for a gTLD domain name or a ccTLD domain name) from using the name to engage in illegal activity. GoDaddy.com LLC is the largest registrar in the world with a market share of 13% and approximately 76 million registrations[181]". GoDaddy serves as a registrar for multiple gTLDs and ccTLDs. In its terms of service, GoDaddy provides: "You represent and warrant to the best of your knowledge that, neither the registration of the domain nor the manner it is directly or indirectly used, infringes the legal rights of any third party"[182].

125. Regarding DNS resolvers, it is important to note that DNS resolver providers – unlike registries and registrars - do not have a (direct or indirect) contractual relationship with the registrant of the domain resolved[183]. Regarding the users of DNS resolvers, practice varies

---

179 usTLD Acceptable Use Policy, Paragraph 1, https://www.about.us/cdn/resources/ebooks/policies/usTLD_Acceptable_Use_Policy.pdf.

180 China Internet Domain Name Regulations: https://govt.chinadaily.com.cn/s/201812/26/WS5c232415498eb4f01ff253d0/china-internet-domain-name-regulations.html.

181 https://domainnamestat.com/statistics/registrar/others.

182 GoDaddy – Domain Name Registration Agreement – last revised 4/5/2022, Section 8 available at: https://www.godaddy.com/legal/agreements/domain-name-registration-agreement.

183 Some DNS resolver providers also provide other services, where they may be in a contractual relationship with the operator of the website. One example is illustrated in the case Court of Appeal (Oberlandesgericht) Cologne of 9 October 2020, 6 U 32/20 – HERZ KRAFT WERKE. Here, "Cloudflare" provided Content Delivery Network (CDN) services to a structurally copyright-infringing website and was sued to stop such services. As "Cloudflare" was also operating a DNS resolver, "Cloudflare" was also sued for an order to

as to the applicability of general terms and conditions. Some DNS resolver providers make it their policy not to provide the DNS resolver services to the user on the basis of general terms and conditions; some even claim that there is no contract at all between the DNS resolver provider and the user[184]. Others seek to impose their general terms and conditions. One example is the "Google Public DNS"[185]. But such general terms and conditions do not set out any specific contractual obligation for the DNS resolver in case the DNS resolver provides access to a copyright-infringing website[186].

c) Enforcement of Contract Terms Related to Copyright Infringement

126. As set forth above, with respect to both gTLDs and ccTLDs contractual terms often exist that obligate domain name registrants to refrain from using domain names in conjunction with copyright-infringing activity. These contractual terms also provide the registrar and the registry the right to suspend/disable and freeze the relevant domain name for violation of the contractual terms. However, enforcement of these contractual terms has been inconsistent at best. For example, as noted by the recent European Commission Study on DNS Abuse, with respect to the contractual provisions in the ICANN accreditation agreements for gTLD registries and registrars related to abuse, "the contractual obligations in place for gTLD registries and registrars (and their resellers, if any) have been found unachieved, ineffective, and/or unenforced by periodic reviews mandated by ICANN Bylaws"[187].

127. A major complicating factor with respect to the willingness of domain name registrars and registries to address (absent a court order) websites engaged in pervasive copyright infringement is the issue as to whether such copyright infringement constitutes "DNS Abuse". The question as to what types of illegal and abusive activity fall within the parameters of "DNS Abuse" and thus should be voluntarily addressed by domain name registries and registrars has been a subject of debate for many years.

128. Often a distinction is made between "technical abuse," which is usually deemed to include the distribution of malware, phishing attacks, botnets, etc. and "content abuse," such

---

cease the resolution of the respective domain of the structurally copyright-infringing website. But the contractual links did not originate from "Cloudflare's" services as a DNS resolver, as "Cloudflare" provided such services independent of any contractual link also for other domains.

184 See for example the DNS resolver provider "quad9": "There is no sign-up, account, or contract to use the service." (https://quad9.net/service/).

185 "By using the Google Public DNS service and its APIs, you consent to be bound by the Google APIs Terms of Service", https://developers.google.com/speed/public-dns/terms.

186 See Google APIs Terms of Service (last modified November 9, 2021):
Section 5: Content, a. Content Accessible Through our APIs – *"Our APIs contain some third party content (such as text, images, videos, audio, or software). This content is the sole responsibility of the person that makes it available. We may sometimes review content to determine whether it is illegal or violates our policies or the Terms, and we may remove or refuse to display content. Finally, content accessible through our APIs may be subject to intellectual property rights, and, if so, you may not use it unless you are licensed to do so by the owner of that content or are otherwise permitted by law. Your access to the content provided by the API may be restricted, limited, or filtered in accordance with applicable law, regulation, and policy*."
Section 7: Privacy and Copyright Protection, b. Google DMCA Policy: *"We provide information to help copyright holders manage their intellectual property online, but we can't determine whether something is being used legally or not without their input. We respond to notices of alleged copyright infringement and terminate accounts of repeat infringers according to the process set out in the U.S. Digital Millennium Copyright Act. If you think somebody is violating your copyrights and want to notify us, you can find information about submitting notices and Google's policy about responding to notices in our Help Center.".*

187 European Commission, "Study on Domain Name System (DNS) Abuse" January 2022 at p. 136 available at https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1.

as the distribution of child sexual abuse material, sale of counterfeit or illegal goods, copyright piracy, hate speech, etc[188]. Many registries and registrars view technical abuse as falling within the parameters of DNS Abuse that they should seek to mitigate by relying on their contractual rights without waiting for court orders or law enforcement actions, whereas they deem content abuse – such as websites devoted to copyright piracy – to fall outside of those parameters. For example, the Council of European National Top-Level Domain Registries ("CENTR") has noted in a policy paper entitled "Domain name registries and online content" that "[w]hether content is illegal or not is a decision for local courts or competent authorities" and that a registry "does not have a special authority to effectively judge the legality of content that is put online"[189]. Similarly the European Commission Study on DNS Abuse observed that, with respect to content abuse, "registries and registrars prefer to simply have to comply with authoritative decisions (i.e., court orders), which provide procedural guarantees and clarity of applicable law"[190].

d) Preventative Actions DNS Service Providers Can Take to Prevent Copyright Infringement

129. While suspending or disabling and freezing the domain name is the only reactive measure that a domain name registry or registrar can take with respect to a website already engaged in copyright piracy, domain name service providers (including registries, registrars, domain resellers, and privacy/proxy service providers) have the ability to undertake a variety of pro-active measures to prevent not only copyright piracy, but online abuse of all kinds. Indeed, a number of these pro-active measures are "neutral" with respect to the type of abuse they help prevent – both technical abuse and content abuse.

130. The European Commission Study on DNS Abuse outlined a number of pro-active measures and good practices that DNS service providers can undertake to prevent abuse of all kinds. These include:

- Registries, registrars, domain name resellers and privacy/proxy services should verify the accuracy of domain name registration data (WHOIS data) that identifies the registrant. This data typically includes the registrant's name, physical address, email address and phone number. Individuals or organizations that intend to operate a website that will engage in illegal activity do not want to share their true identifying information to obtain a domain name. Therefore, if domain name service providers verify the accuracy of this information and refuse to register a domain name to a person or organization that supplies false or inaccurate information, then this deters abuse of all kinds. Clear evidence of this positive impact with respect to websites engaged in IP infringement exists. For example, when DK Hostmaster, the registry for Denmark's .dk ccTLD, undertook more rigorous measures to confirm the identity of its domain name registrants – both legal and natural persons – beginning in November 2017, it resulted in an 85% decrease in websites operating under the .dk ccTLD suspected of IP rights

188 See e.g., Internet & Jurisdiction Policy Network, "Toolkit DNS Level Action to Address Abuses" March 2021 at p. 5, 13-14: https://www.internetjurisdiction.net/domains/toolkit.
189 CENTR, "Domain Name registries and online content" January 2019 at pp. 11-12: available at https://centr.org/library/library/policy-document.html.
190 European Commission, "Study on Domain Name System (DNS) Abuse" January 2022 at p. 131 available at https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1.

infringement (from 6.73% to 1.03%) in just four months[191]. Thus the European Commission Study recommends that accuracy requirements be imposed on all DNS service providers and notes that "accuracy can be obtained by strict registrant identification, e.g., through Know Your Business Customer ("KYBC") procedures and cross-checks in publicly available data bases"[192]. The European Commission Study describes in detail the various procedures adopted by a number of registries and registrars to undertake this verification, including the processes adopted by EURid, the registry for the .eu ccTLD[193].

Some countries – for example the Republic of Korea - have even introduced legislation that allows the domain providers to request the registrant to submit information which can identify the registrant. When information which helps to identify the registrant turns out to be false, the domain provider shall cancel domain names (Article 11 Korean Internet Address Resources Act).

- The use of predictive algorithms and artificial intelligence to identify and prevent abusive domain name registrations. For example, the European Commission Study describes the predictive algorithm used by EURid called the Abuse Prevention and Early Warning System (APEWS)[194].

- The use of blacklists, such as those produced by Spamhaus, the Anti-Phishing Working Group (APWG), and OpenPhish[195].

- The monitoring by registries of the levels of abuse seen in the registrations made by their various registrars and providing financial incentives to those registrars with low levels of abuse and financial penalties to – and perhaps even terminating accreditation of – registrars with high levels of abuse[196].

131. In March 2021, the European Union Intellectual Property Office (EUIPO) published a discussion paper entitled "Domain Names: Challenges and good practices from registrars and registries to prevent the misuse of domain names for IP infringement activities"[197]. The Paper identifies a number of pro-active and preventative measures that domain name service providers can undertake to help prevent the registration and use of domain names associated with IP infringement. The measures identified are:

- Including terms and conditions in the agreements between registries and registrars and between registrars and domain name registrants that clearly

191 European Commission, "Study on Domain Name System (DNS) Abuse" January 2022 at pp. 158-59 available at https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1. The .dk registry is now required by law, on notice of a reasonable suspicion that WHOIS data is inaccurate, to verify the WHOIS record and to correct it or suspend the domain within 30 days: Article 15, Executive Order on the Internet Domain .dk, BEK no. 44 of 14/01/2020.

192 Ibid.at p. 135.

193 Ibid. at pp. 152-55.

194 Ibid.at pp. 152-54.

195 Ibid. at p. 16, pp. 165-66 and Appendix 1-Technical Report at pp. 22-24.

196 Ibid at p. 16.

197 EUIPO, Domain Names – Discussion Paper "Challenges and good practices from registrars and registries to prevent the misuse of domain names for IP infringement" March 2021: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Discussion_Paper_on_Domain_Names/2021_Discussion_Paper_on_Domain_Names_FullR_en.pdf.

identify IP rights infringement as a breach of contract that can lead to suspension of the domain name.

- Prohibiting or limiting the use of privacy and proxy services.
- Implementing alert systems and rights protection mechanisms to inform trademark owners of the application for or registration of a domain name identical to their trade mark in order to object to the application/registration.
- Implementing systems to verify the identity of the registrant (i.e., the WHOIS data of the registrant), using electronic identification solutions, and/or public registries and refusing to register domain names if the registrant/WHOIS data is inaccurate or false.
- Implementing systems to monitor and automatically detect abusive domain name registration applications and suspend and/or reject the applications.
- Implementing post-registration manual and/or automated checks to look for incorrect or seemingly false WHOIS data and suspending domain names if the registrants do not provide evidence correcting/verifying the WHOIS data.

132. All of the pro-active and preventative measures and good practices identified and described by the European Commission Study and the EUIPO Discussion Paper have been implemented individually or collectively by a number of ccTLD and gTLD registries and registrars.

133. As the EUIPO Discussion Paper correctly observes, "the domain name holders for websites engaging in illegal activities rarely use their real contact details and would typically not react to a verification request"[198]. Thus, for registries and registrars that perform verification on the information supplied by applicants and registrants for domain names and decline to register and/or suspend domain names for registrants supplying incomplete, inaccurate or false contact information, this acts as a powerful tool to combat illegal activity of all kinds, including copyright piracy. Indeed, as stated by the EUIPO Discussion Paper "It can even be more efficient and less burdensome than requesting the deletion of single domains for IP-infringing activities, as failure to comply with one verification request may result in the deletion of all the domain names of a specific domain name holder [registrant]"[199].

134. As of June 2022, a Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (commonly referred to as "NIS-2") has been subject to inter-institutional discussions among the European Parliament, the Council and the European Commission. According to the current compromise language of NIS-2 found at Article 23, domain name registries, registrars and other entities providing domain name registration services (such as privacy or proxy service providers) would be required to "collect and maintain accurate and complete domain name registration data in a dedicated database" and "have policies and procedures in place to ensure that the databases include accurate and complete information, including verification procedures"[200].

198 Ibid. at p. 27.

199 Ibid.

200 Interinstitutional File: 2020/0359 (COD) 3 June 2022 available at : https://politico-uploads-production.s3.eu-west-1.amazonaws.com/editorial_documents/d5197aea-f226-44e3-b747-27ce89ae25d4-Proposal%20for%20a%20DIRECTIVE%20OF%20THE%20EUROPEAN%20PARLIAMENT%20AND%20OF%20THE%20COUNCIL%20on%20measures%20for%20a%20high%20common%20level%20of%20cybersecurity%20across%20the%20Union.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-

135. Although the NIS-2 Directive Proposal is still being finalized and needs to be voted on by the European Parliament, it is likely to be adopted sometime before the end of 2022. Once adopted, the EU Member States will have 21 months to transpose the Directive into their national laws. Assuming the language of Article 23 remains unchanged, then by law registries, registrars, privacy or proxy services, and domain name resellers offering their TLDs or services to residents of EU Member States will be required by law to ensure that the registration information/WHOIS data of their registrants is accurate and verified. As explained in the European Commission Study on DNS Abuse and the EUIPO Discussion Paper, such accuracy and verification practices – if implemented and enforced – should lead to reductions in websites engaging in illegal activities, including copyright infringement.

IV. VOLUNTARY MEASURES UNDERTAKEN BY DNS SERVICE PROVIDERS TO ADDRESS COPYRIGHT INFRINGEMENT

136. ICANN requires both registries and registrars to maintain arrangements to deal with abuse of domain names managed by them, but "abuse" is not comprehensively defined in those agreements[201]. As ICANN has observed, "[t]he ICANN community has not yet reached a consensus definition for 'DNS Abuse'"[202]. Outside the context of judicial enforcement, the question arises whether copyright infringement through use of a domain name should be regarded as DNS abuse for the purposes of the practices of DNS service providers.

137. In 2019, a group of registries and registrars created a Framework to Address Abuse[203]. The Framework now has nearly 50 registries and registrars that have signed on to it. This Framework defines DNS Abuse as "composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam (when it serves as a delivery mechanism for the other forms of DNS Abuse)." The Framework states that registries and registrars "must act upon these categories of DNS Abuse" when identified and acknowledges that the "only mitigation tool a registry or registrar possesses is to disable the entire domain name." The Framework goes on to state that registries and registrars frequently receive complaints about a website's content, where that website is operating under a domain name that is administered by the registry or has been registered by the registrar. The Framework refers to this type of abuse as "Website Content Abuse" and maintains that this type of abuse is distinct from DNS Abuse. According to the Framework, "acting at the DNS level to address Website Content Abuse in general is a disproportionate remedy." Nevertheless, the Framework identifies four categories of Website Content Abuse that it describes as "so egregious that a registry or registrar *should* act when provided with specific and credible notice" and not require a court order to do so. The four categories identified are: (1) child sexual abuse materials; (2) illegal distribution of opioids online; (3) human trafficking; and (4) specific and credible incitements to violence[204].

Credential=AKIA4OBOTACJP5YG7GJL%2F20220621%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20220621T051809Z&X-Amz-Expires=10&X-Amz-SignedHeaders=host&X-Amz-Signature=dcc9f6587bf8b0d592ebff4e84cff496a446bc407eeeedf7e7babebf112247a8.

201 For registries, see section 4.1 "Abuse contact", Specification 6, Base Registry Agreement (2017). For registrars, see section 3.18 "Registrar's Abuse Contact and Duty to Investigate Reports of Abuse", Registrar Accreditation Agreement (2013) and Specification on Privacy and Proxy Registrations, sections 2.2 and 2.4 (obligations of proxy or privacy service providers).

202 "DNS Security Threat Mitigation Program", ICANN website https://www.icann.org/dns-security-threat, accessed May 4, 2022.

203 https://dnsabuseframework.org/.

204 https://dnsabuseframework.org/media/files/2020-05-29_DNSAbuseFramework.pdf.

138. Under the terms of the Framework, even when a website is devoted to copyright piracy on a commercial scale or is a structurally copyright-infringing website, this type of content abuse does not merit a registry or registrar taking action to disable/suspend the domain name of the website without a court order of proper jurisdiction. The Framework maintains that the "line between free expression and illegal content varies across jurisdictions, cultures and even changes over time"[205]. While that statement and justification certainly has merit in many contexts concerning content, it neglects the fact that wholesale copyright infringement of entire works is regarded as illegal activity across the globe. Indeed, 179 states are currently members of the Berne Convention for the Protection of Literary and Artistic Works that provide authors and creators exclusive rights concerning the exploitation of their creative works[206].

139. In January 2022, the European Commission published a detailed and extensive "Study on Domain Name System (DNS) Abuse". Agreeing with ICANN, this Study finds that "consensus on a global and comprehensive DNS abuse definition is still missing"[207]. The Study rejects a rigid distinction between technical abuse and content abuse. Instead, the Study adopts the following definition:

> "Domain Name System (DNS) abuse is any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity"[208].

140. Under this definition, a website engaged in copyright piracy operating under a domain name is committing DNS abuse. Indeed, the Study has an entire section devoted to Intellectual Property Rights Infringements, including illegal sharing and distribution of copyright protected works[209]. The Study notes that organized crime groups are heavily involved in online copyright piracy and counterfeiting, and that intellectual property crime is often combined with other types of crime.

141. Once a website is operational and functioning under a particular domain name, the only remedy that is within the technical capability of a domain registry or registrar to mitigate abuse (however defined) that is emanating from that website is to disable or suspend the domain name and freeze the domain name to prevent it from being transferred to another party. As stated in the Framework to Address Abuse, registries and registrars do not have the technical ability surgically to target abusive parts or particular pages or URLs of a website. Thus, when a domain name is suspended, practically speaking the entire website associated with that domain name, including all the content on the website, any sub-domains and associated emails, is disabled.

142. As set forth in Section III above, courts can order the suspension and seizure of domain names in cases involving websites engaged in copyright infringement. However, some registries have engaged in voluntary cooperative efforts to address websites engaged in pervasive copyright infringement operating under domain names that these registries administer. These cooperative efforts typically involve arrangements known as "trusted notifier" or "trusted flagger" agreements. Under these arrangements, the registry works with an organization that has knowledge and deep expertise in identifying websites engaged in pervasive copyright infringement. That organization is the notifier or flagger. When it finds a

---

205 Ibid.

206 https://www.wipo.int/treaties/en/ip/berne/.

207 European Commission, "Study on Domain Name System (DNS) Abuse" January 2022 at p. 10 available at https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1.

208 Ibid.

209 Ibid. at paras. 73-80.

website engaged in pervasive copyright infringement operating under a domain name administered by the registry, the notifier/flagger will send a written notice to the registry identifying the website and domain and supplying evidence. Often under these arrangements, the notifier/flagger will be required to first contact the hosting provider of the website and the registrar of the domain name to seek redress (i.e., the stopping of hosting of the website by the hosting provider – thus taking the website offline; the suspension of the domain name of the website by the registrar). If the notifier/flagger receives either a negative or no response from the hosting provider and registrar, then the registry will consider the notifier/flagger's written notice and make a decision to suspend the domain name.

143. In practice, trusted notifier/flagger arrangements have been employed more frequently to address websites engaged in the sale of illegal opioids or distribution of child sexual abuse materials than with respect to copyright piracy and have been put in place with both registries and registrars. The registry/registrar authored Framework to Address Abuse recognizes the value of trusted notifiers in those two particular categories of website content abuse. As stated in the Framework, "Trusted Notifiers earn the registries' and registrars' trust with a recognized subject matter expertise, an established reputation for accuracy, and a documented relationship with and defined process for notifying the registries and registrars of alleged abuse. While it is ultimately the responsibility of the registries and registrars to take action on verified forms of abuse, Trusted Notifiers can serve as a crucial resource"[210].

144. Two major gTLD registries, Donuts and Radix, have entered into trusted notifier arrangements to address websites engaged in pervasive copyright infringement. The European Commission Study on DNS Abuse describes the various trusted notifier arrangements that Donuts has in place to address not only copyright infringement, but also child sexual abuse material. The Study notes that Donuts has trusted notifier arrangements in place with both the Motion Picture Association and ("MPA") and the Recording Industry Association of America ("RIAA") to address copyright infringement[211]. The trusted notifier arrangement between Donuts and the MPA was announced in February 2016 and is still operational[212]. Donuts is the registry for the largest number of new gTLDs and serves as the registry for more than 240 gTLDs[213]. Approximately one year following the announcement of the trusted notifier arrangement, the MPA issued a press release reporting on the success of the arrangement with affirmation from Donuts[214]. The release explained that pursuant to the trusted notifier arrangement, action was taken with respect to the domain names of 11 websites engaged in large-scale copyright piracy during the first year of the collaboration. As stated in that announcement, Donuts and MPA jointly published a high-level description of their trusted notifier arrangement entitled "Characteristics of a Trusted Notifier Program". That document is attached to this paper as Annex 1.

145. Approximately three months following the announcement of the trusted notifier arrangement with Donuts, a joint announcement was made by Radix and the MPA in May 2016 of a trusted notifier relationship to address online copyright piracy[215]. Radix is based in

---

210 Framework to Address Abuse, available at: https://dnsabuseframework.org/.

211 European Commission, "Study on Domain Name System (DNS) Abuse" January 2022 at p. 146 available at https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1.

212 https://www.motionpictures.org/wp-content/uploads/2016/02/Donuts-and-MPAA-Establish-New-Partnership-2.9.16.pdf.

213 https://donuts.domains/what-we-do/top-level-domain-portfolio/.

214 https://www.motionpictures.orgs/press/one-year-later-trusted-notifier-program-proves-effective/.

215 https://www.prnewswire.com/news-releases/radix-and-the-mpaa-establish-new-partnership-to-reduce-online-piracy-579359971.html.

the United Arab Emirates and serves the registry for such gTLDs as .online, .website and .store[216]. As is the case with Donuts, the trusted notifier arrangement between Radix and the MPA continues to operate.

146. With respect to ccTLDs, in 2018 EURid, the registry for the .eu ccTLD, announced that it had entered into a Memorandum of Understanding with the International Anti-Counterfeiting Coalition (IACC) to exchange information and collaborate in addressing counterfeiting and piracy[217]. While it is not clear whether this arrangement includes the elements of trusted notifier with respect to specific websites and domain names, it is another positive example of voluntary cooperation between domain name registries and organizations with expertise in IP rights infringement to combat this illegal activity.

147. In 2017, in its Communication concerning Tackling Illegal Content Online, the European Commission noted that "trusted flaggers can be expected to bring their expertise and work with high quality standards". Thus the Commission "encourages the close cooperation between online platforms and trusted flaggers […]. This cooperation should provide for mutual information exchange so as to evaluate and improve the removal process over time"[218]. The EUIPO Discussion Paper of 2021 also highlighted trusted notifier arrangements in the context of the domain name system to address IP infringement[219]. The 2022 European Commission Study on DNS Abuse sets forth as one of its key 27 recommendations "to require DNS service providers to collaborate with […] so-called trusted notifiers and trusted flaggers"[220]. The concept is incorporated in the European Commission's proposal for a Digital Services Act. Under the common position agreed on June 15, 2022, notices submitted to "providers of online platforms" (essentially, hosting providers making information available to the public) by trusted flaggers are to be "processed and decided upon with priority and without undue delay"[221].

148. The overwhelming majority of the world's countries are signatories to the Berne Convention for the Protection of Literary and Artistic Works and, therefore, recognize the rights of authors in their literary and artistic works. Standards for evaluating copyright infringement involving the wholesale unauthorized exploitation of entire copyrighted works by infringing websites do not significantly vary or conflict. Such pervasive copyright infringement is internationally recognized as illegal activity. Therefore, trusted notifiers can be employed at global level to assist domain name service providers (as well as other online intermediaries) to cease providing services, including suspending and freezing domain names, with respect to websites engaged in wholesale copyright infringement.

---

216 https://www.ascio.com/blog/radixs-tlds-continue-to-be-strong-performers/.

217 https://eurid.eu/en/news/eurid-and-iacc-team-up-to-fight-cybercrime/.

218 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, "Tackling Illegal Content Online: Towards an enhanced responsibility of online platforms", COM(2017) 555 final, September 2017 at pp. 8-9: https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2017)555&lang=en.

219 EUIPO, Domain Names – Discussion Paper "Challenges and good practices from registrars and registries to prevent the misuses of domain names for IP infringement" March 2021 at pp.30-31: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Discussion_Paper_on_Domain_Names/2021_Discussion_Paper_on_Domain_Names_FullR_en.pdf.

220 European Commission, "Study on Domain Name System (DNS) Abuse" January 2022 at p. 18 available at https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1.

221 See Article 19, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM/2020/825 final). See common position, as set out in Council of the European Union, document no. 14124/20 + ADD 1-3, June 15 2022, available at https://data.consilium.europa.eu/doc/document/ST-9342-2022-INIT/x/pdf.

V. CONCLUSIONS

149. The legal frameworks for the participation of DNS service providers in enforcement activities against online copyright infringement are in a state of development. As shown above, case law regarding registries and registrars lacks a clear picture at international and national levels. National jurisprudence on the potential liability of such operators as primary or secondary infringers and the relevance of the "safe harbors" arising under electronic commerce legislation remains limited.

150. At the same time, as discussed above, there are remedies not based on liability (i.e., no-fault injunction orders) which have proved successful in many countries and which could be applicable in the case of DNS service providers, depending on national law. In considering any non-fault duty for DNS service providers, the principle of proportionality should evidently be applicable[222]. It is necessary to balance-out the conflicting fundamental rights by all parties involved. As shown above in detail for DNS blocks, it is in particular necessary to find an adequate balance between the fundamental right to property (copyright holder), fundamental right to conduct a business (DNS service provider) and the right to access information (Internet user)[223].

151. In the area of copyright, remedies against DNS service providers are in particular sought by right holders in cases of domain names that are used for structurally copyright-infringing websites, i.e., for websites which follow a copyright-infringing business model, systematically generating copyright infringements (so-called structurally copyright-infringing websites)[224]. As described in this study, under no fault injunctive relief, for example, registries and registrars could be obliged to disable such websites' domain names, and registrars could also freeze them (the registrar must also not participate in transferring the domain to another registrar). DNS resolver providers have been obliged by courts not to resolve the respective domain names of such websites.

152. Legal duties, which are not based on infringement, have been introduced in some countries, to address the anonymity of site operators, a familiar obstacle to online enforcement. As discussed above, verification of the accuracy of the contact and identification information of registrants, as in Denmark with respect to the .dk ccTLD, is a powerful tool that prevents abusive and illegal activity of all kinds, including copyright infringement. The NIS-2 Proposed Directive, if adopted in accordance with its current compromise language, will create legal obligations across the member states of the EU to require accuracy and verification of domain registrants' contact and identification information. The imposition of a duty upon Internet intermediaries to forward notices of infringement to account holders is a further possible measure as in Canada with respect to the access and hosting providers.

153. Beyond judicial enforcement, there are various examples of voluntary cooperation between right holders and DNS service providers, based on the acceptable use policies of these parties. Registries and registrars are connected to the infringer via contractual relationships. The infringer either has a direct contract with the registrar or is in an indirect contractual relationship via resellers to a registrar or registry. It would assist in developing

222 In accordance with Article 7, Agreement on Trade-related Aspects of Intellectual Property Rights (TRIPS Agreement).
223 See also Schwemer, Location, Location, Location! Copyright Content Moderation at Non-Content Layers, p. 393, in Rosati, Routledge Handbook EU Copyright Law, 2021.
224 See para. 84 above.

such cooperation if consensus could be reached on an inclusive definition of DNS abuse and it were made clear under the contractual terms of both registries and registrars that the use of domain names to commit copyright infringement constitutes a category of such abuse.

154. The concept of trusted notifier arrangements to address illegal behavior online seems to be growing in prominence, with legislative developments pending in the EU. These arrangements can be with law enforcement agencies, government agencies or departments with copyright expertise or with private organizations with relevant knowledge and expertise concerning copyright infringement.

155. Given the centrality of DNS operators and service providers to the functioning of the Internet, there will no doubt continue to be further innovation in the legal and extra-legal means available for tackling online copyright infringement through the DNS.

ANNEX 1: CHARACTERISTICS OF A TRUSTED NOTIFIER PROGRAM

Trusted Notifier Status

- The Registry must be willing to accept and act on referrals received from the Trusted Notifier. As such, it is important for the Trusted Notifier to be a recognized authority within the field in which it operates.
- Characteristics of a Trusted Notifier include an industry representative trade association that represents no single company, a recognized not-for-profit public interest group dedicated to eliminating illegal behavior, or a similarly situated entity with demonstrated extensive expertise in the area in which it operates and ability to identify and determine the relevant category of illegal activity.
- The Trusted Notifier must be willing to stand behind its referrals.
- The relationship is voluntary in nature – either party may withdraw from the program at any time.

Operations

- Both the Registry and Trusted Notifier provide designated points of contact for the sending and receiving of referrals regarding abuse in a TLD.
- The Trusted Notifier's referrals will be treated expeditiously and with a presumption of credibility, though the Registry may conduct its own investigation.

Standards for Referrals

Referrals from the Trusted Notifier must include, at a minimum, a:

- statement that the Trusted Notifier is authorized to submit the referral (e.g. for copyrights, the Trusted Notifier has authority to assert a claim on behalf of the right holder);
- detailed description of the abusive activity (i.e., sample URLs, screen shots);
- non-exhaustive Identification of the law(s) being violated by the activity;
- clear and brief description of why the site's activity violated the specified law(s);
- statement that, prior to sending the referral, the Trusted Notifier alerted or attempted to alert the registrar of record and hosting provider, including a description of the response received, if any, from registrar and hosting provider and an explanation of why such responses failed mitigate the abuse;
- statement that the referral is submitted with a good faith belief that the information contained therein is true and accurate; and
- confirmation that the referral was subject to careful human review by the Trusted Notifier – not submitted solely based on automated Internet scanning or scraping services.

In addition to satisfying all of the elements above, before submitting a referral, the Trusted Notifier will make a good faith effort to determine whether the domain is operating with false WHOIS information.* Where applicable, the referral will also include the following to the best of Trusted Notifier's knowledge:

- statement that WHOIS information provided by the registrant contains false or misleading information; and
- identification of which WHOIS field may be false or misleading.

Actions by the Registry

- Registry will review the referral on an expedited basis.
- Registry will coordinate with the applicable registrar.
- As appropriate, registrar (or Registry if registrar declines) may provide the referral to the registrant, and will set a reasonable deadline in which to receive a response.
- If Registry agrees that the domain clearly is devoted to abusive behavior as reported in the referral, the Registry, in its discretion, may suspend, terminate, or place the domain on registry lock, hold, or similar status as it determines necessary to mitigate the harm and that such action may constitute an appropriate response to a domain engaged in clear and pervasive abusive behavior.
- If the Registry has concerns, questions the scope or nature of the reported abuse, or has received alternative instruction from law enforcement or similar authority, the Registry should provide a written explanation promptly to the Trusted Notifier and give the Trusted Notifier opportunity to supplement or amend its referral.
- Absent exceptional circumstances, the Registry will endeavor to determine a course of action and inform the Trusted Notifier of its decision within 10 business days of receipt of the referral.

*NOTE: The requirements concerning making a good faith effort to determine whether the domain is operating with false or misleading WHOIS information were operative when all WHOIS data for all generic top-level domains was publicly accessible. Since May 2018, in accordance with ICANN's Temporary Specification, most of this information is no longer publicly accessible. Therefore, these requirements/components of the Trusted Notifier arrangement have not applied since May 2018 and the notifier is no longer required to make a good faith determination concerning the nature of the WHOIS information because the notifier does not have ready access to such information.

World Intellectual Property Organization
34, chemin des Colombettes
P.O. Box 18
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 338 91 11
Fax: + 41 22 733 54 28

For contact details of WIPO's
External Offices visit:
www.wipo.int/about-wipo/en/offices