10 MARCH 2018 (Author's Original Version)

On Domain Registries and Website Content

Shift in Intermediaries' Role in Light of Unlawful Content or just another Brick in the Wall?

Sebastian Felix Schwemer [*] [†]

Original place of publication: Sebastian Felix Schwemer, "On domain registries and unlawful website content: Shifts in intermediaries' role in light of unlawful content or just another brick in the wall?" *International Journal of Law and Information Technology*, Volume 26, Issue 4, 1 December 2018, Pages 273–293, https://doi.org/10.1093/ijlit/eay012

Abstract

The link of lawful domain names to unlawful content is a phenomenon that has not been very topical until recently. Traditionally, domain registries have been off the radar of content-related debates. Enforcement efforts, public discourse and academic research have focused on other intermediaries such as Internet access service providers, hosting platforms, and websites that link to content.

This article shows that in recent years, however, that the (secondary) liability of domain registries and registrars, and more specifically country code top-level domain (ccTLD) registries for website content, has been tested in several EU Member States. The article investigates tendencies in the national lower-court jurisprudence and explores to what extent the liability exemption regime of the E-Commerce Directive applies to domain registries. The analysis concludes that whereas domain registries can be read under the exemptions in a teleological interpretation, more clarity is desirable.

Keywords: DNS governance, ccTLD regulation, liability, content regulation, governance-by-infrastructure
JEL: K24, L68, O34

[*] Ph.D., Industrial PostDoc, Centre for Information and Innovation Law (CIIR), University of Copenhagen and Danish Internet Forum (DIFO).

[†] Acknowledgements: this article is part of a research project that has been funded by the Danish Innovation Fund and the Danish Internet Forum (DIFO). I thank Professor Thomas Riis, Head of Legal Department Henriette Vignal-Schjøth, Professor Lee Bygrave and Professor Tobias Mahler for their comments on a draft of this paper. This research represents solely the view of the author. The author enjoyed full academic freedom, but acknowledges that the research results may be in the interest of the co-funding organization.

Contents

1. Introduction

Intermediaries are the focal point in the functioning and the governing of the Internet.[1] In the fight against unlawful or unwanted content on the Internet, the role of some of these intermediaries has been debated since the very early days of the Internet. In the course of the last decade, cybersecurity, and related to this, cybercrime, has become more prevalent in policy- and lawmaking. Enforcement efforts and public discourse have been especially focused on the role of Internet access service providers, hosting platforms, and websites that link to content. In academic research, too, these intermediaries and their legal role and responsibility are a well-studied phenomenon.

The domain name system (DNS), on the other hand, has received comparably little attention in the discussion of online content. Recent developments, however, point towards a more prominent role of domain names and their administration in Internet governance and more specifically content control online. In September 2017, for example, Spanish authorities requested the .cat-registry to "block" access to all websites containing content on an upcoming independence referendum.[2] This is just one of many examples, where domain names become topical when looking at content online. In some of these instances, public opinion might support such policing measures (think of child pornography or terror propaganda), whereas calls for a more careful balance with fundamental freedoms are heard in other instances. This leads to a debate on the very foundation and principles of the role and liability of domain registries as intermediaries.

As research subject, domain names have had a first peak in the late 1990s leading up to the dot-com bubble. Today, there exists a vast legal literature focusing on the

[1] In some instances, private organisations as intermediaries are argued to act akin to governments as de facto regulators. See e.g. Jaani Riordan, *The Liability of Internet Intermediaries* (OUP 2016), 354.

[2] See e.g. Jonah Engel Bromwich, 'Spain and Catalonia Wrestle Over .Cat Internet Domain' (*The New York Times*, 22 September 2017) <https://www.nytimes.com/2017/09/22/style/cat-domain-catalonia.html> accessed 15 January 2018.

institutional setup or the lawfulness of domain names *as such*.[3] Computer scientists have covered various topics such as the detection of algorithmically generated malicious domain names.[4] Economists, too, have started endeavours into describing and quantifying domain-name related online crimes such as phishing.[5] The link of (lawful) domain names to unlawful content, on the other hand, is a phenomenon that has only relatively recent become prevalent and there exists little research on the topic. Compared to other intermediaries, the role of domain registries, it appears, has been neglected as legal research subject – despite their function as crucial infrastructure. Likewise, questions regarding legal obligations of this specific intermediary remain largely unaddressed in the literature.[6] One explanation for this neglect could be seen in the relatively recent trend of involving domain registries in content regulation and enforcement. Thus, the legal role and liability of top-level domain registries regarding the content associated with domain names is to a large degree unknown. This article contributes to clarifying these questions with focus on European country code top-level domain registries (ccTLDs).

In the following, I first provide a general overview of the functioning of the top-level domain administration system and the current state of regulatory affairs to set the scene. Then, I look towards liability and liability exceptions for domain registries. Compared to registries, other intermediaries, such as Internet access service providers or online platforms, have been longer in the crosshair. In the absence of DNS-specific regulation, I draw on a horizontal analysis of the functioning of other intermediaries and their role and responsibility regarding unlawful content. Ultimately, this article aims to contribute to understanding shifts in content policing and the underlying question of whether domain registries play a role, and if so, what it looks like, can be or ought to be.

2. Functioning and regulatory characteristics of the domain name system

a) Functioning and actors

The operations of the Internet and its content depend on a variety of infrastructure services, which are offered by different intermediaries, such as Internet access service

[3] See e.g. Torsten Bettinger and Allegra Waddell (eds), *Domain Name Law and Practice* (OUP, 2nd edn, 2015). In 2017, for example, the European Intellectual Property Office (EUIPO) published research on suspected trade mark infringing e-shops utilising previously used domain names.

[4] Sandeep Yadav et al., 'Detecting Algorithmically Generated Malicious Domain Names' (2010) IMC '10, 48–61.

[5] Tyler Moore et al., 'The Economics of Online Crime' (2009) 23 Journal of Economic Perspectives, 3–20.

[6] See however M. Truyens and P. Van Eecke, 'Liability of domain name registries: Don't shoot the messenger' (2016) 32 Computer Law & Security Review, 327–334; Brenden Kuerbis, Ishan Mehta, Milton Mueller, 'In Search of Amoral Registrars: Content Regulation and Domain Name Policy' (2017) Internet Governance Project White Paper; Annemarie Bridy, 'Notice and Takedown in the domain name System: ICANN's Ambivalent Drift into Online Content Regulation' (2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2920805> accessed 15 January 2018. David G. Post 'Internet Infrastructure and IP Censorship' (2015) IP JUSTICE JOURNAL: Internet Governance and Online Freedom Publication Series. This observation is not restricted to the legal perspective; the study of ccTLDs and their governance has also been labelled as a "field very much under-addressed by political scientists", see George Christou and Seamus Simpson, 'New Modes of Regulatory Governance for the Internet? Country Code Top Level Domains in Europe (European Consortium for Political Research General Conference, Pisa, September 2007) 10.

providers, hosting providers, platforms or DNS-service providers.[7] The OECD defines Internet intermediaries as follows:

> "Internet intermediaries bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties."[8]

This article does not prerequisite a deep understanding of the technical functioning of these intermediaries. Nonetheless, it is crucial to have a basic understanding of the technical DNS-setup, in order to understand the possibilities and implications of interfering in the DNS (e.g. at the registry, registrar or server level).

The DNS is the technical protocol for the organisation of the global name space and remains in its principles unchanged since it was taken into use in the 1980s. On the European level, only recently a regulatory instrument addressed the functioning of the DNS for the first time.[9] Article 4 nr. 14 of Directive 2016/1148/EU (NIS Directive)[10], which has to be implemented by Member States by 9 May 2018, defines the "domain name system" as a "hierarchical distributed naming system in a network which refers queries for domain names". The traditional narrative compares the DNS to a telephone book: the addresses of servers, in the form of a string of numbers as Internet Protocol (IP) addresses, are being connected to domain names, which make them easier to access and remember.[11] A top-level domain (TLD) is the highest name in the hierarchical name space, today consisting of approximately 200 TLDs that refer to countries, known as country-code TLDs (ccTLDs) such as .de, .dk or .se, and a large number of generic TLDs (gTLDs), such as .com, .edu or .org. Following a major expansion in 2012, there are currently more than 700 gTLDs in use and almost 2.000 gTLDs on a wait list. Interestingly, in the 1990s it was deemed "extremely unlikely" that additional gTLDs would be added.[12] Notably, the usage of these new gTLDs seems to differ and researchers found that "only 15 % of domains in the new TLDs show characteristics consistent with primary registrations, while the rest are promotional, speculative, or defensive in nature".[13]

---

[7] A word on the notion of internet service providers (ISP): various intermediaries are often referred to as Internet service providers, both in academic research and everyday usage, a notion that misses sharpness because it does not differentiate between the underlying function, e.g. hosting of content or providing Internet access. I thus refrain from imposing a unitary terminology beyond "intermediary" for the sake of this article.

[8] Organisation for Economic Cooperation and Development (OECD), 'The Economic and Social Role of Internet Intermediaries' (OECD, 2010), 9. The report stipulates the goal "to ensure that the definition used by the OECD is comprehensive and accurate".

[9] The top-level domain space for the .eu ccTLD has been regulated since 2002.

[10] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19 June 2016, 1–30.

[11] *Riordan* (2016) speaks of a translation into "human-friendly" names, 39.

[12] See also RFC 1591: Domain Name System Structure and Delegation (author: J. Postel) (March 1994) <https://tools.ietf.org/html/rfc1591> accessed 15 January 2018. On the conceptual challenges see Tobias Mahler, 'A gTLD right? Conceptual challenges in the expanding internet domain namespace' (2014) 22 International Journal of Law and Information Technology, 27–48.

[13] Tristan Halvorson et al., 'From .academy to .zone: An Analysis of the New TLD Land Rush' (IMC 15 Proceedings of the 2015 Internet Measurement Conference) 381–394.

DNS-functions are performed by different actors. Article 4 nr. 15 of the NIS Directive stipulates "DNS service provider" tautologically as "an entity which provides DNS services on the internet". The intermediaries responsible for domain names are registry operators, which "control the registration and resolution of domain names within a particular namespace".[14] Article 4 nr. 16 of the Directive defines "top-level domain name registry" as "an entity which administers and operates the registration of internet domain names under a specific top-level domain (TLD)". The core operations of these registries include the operation of name servers and the WHOIS database (containing information about domain names, registrants and servers) as well as setting guidelines for the allocation, registration, deletion and transfer of domain names under their specific top-level domain(s). Thus, (top-level) domain registries perform essential services in the digital infrastructure sector, that are also recognised by the European lawmaker.[15] From domain registries one needs to differentiate registrars, which "accept[s] registrations from third parties for a domain name, reserve[s] that domain name in the relevant registry, and permit[s] registrants to manage its configuration, in return for payment of an annual fee".[16] Thus, registrars act akin to retailers and in some instances provide additional services such as hosting.

When talking about domain name-related remedies, many different terminologies such as "take-down" or "blocking" are regularly used to describe the result of rendering a website inaccessible via a domain name. There exists no apparent consensus on the duration (temporary or permanent) of these measures. Additionally, these notions do not directly translate to the operational reality of registries. From their point of view, remedies can commonly be differentiated among deletion (disconnection of the domain name to name servers and de-registration of the domain name in the registry database; i.e. the domain name becomes available for new registrants), suspension (domain name is temporarily disconnected from name servers but remains registered), transfer to a different registrant (right to use a domain name goes to another natural or legal person, e.g. the state), or blocking (prevention of registration of the domain name for present and future use; i.e. domain name cannot be connected to name servers). Given the lack of a coherent usage or definition in the sparse literature or case law, I propose to understand "take-down" of domain names for the sake of this article as revocation of the right to use a domain name by a registrant, consisting of any of the above-mentioned measures.

b) Governance and regulatory characteristics

Conventionally, the DNS has operated on the fringes of traditional regulation in form of secondary legislation. In fact, on a global scale, the domain name vertical has been rarely touched upon by state-enacted law.[17] Instead, the institutional framework is for historical

[14] *Riordan* (2016) 39.

[15] According to Annex II to the NIS Directive, "TLD name registries" (in the digital infrastructure sector) are entities for the purpose of point (4) of Article 4 of the Directive, meaning an "operator of essential services", which meet the criteria laid down in Article 5(2).

[16] See *Riordan* (2016) 198. The setup can vary, as for example in Denmark.

[17] See also Jens Schovsbo, 'The private legal governance of domain names' in Thomas Riis (ed), *User Generated Law* (Edward Elgar 2016) 206–227. This is somewhat counterintuitive given that domain names constitute what is akin to a natural monopoly. In these markets, regulation is by economic theory argued to be crucial "ensure

reasons enshrined in non-state actors and organised in form of self-governance with great reliance on a "contractual web".[18] The non-profit organization Internet Corporation for Assigned Names and Numbers (ICANN), which was established in 1998, acts *inter alia* as coordinator and central repository for the IP addresses and the management of the principal DNS root.[19]

In the case of ccTLDs, registries are regularly working in the public interest. When looking at ccTLDs in Europe, there is a varying level of regulation and state-involvement, which might also affect liability. Acknowledging these differences is important for understanding that the playing field is maybe not as level as it seems.[20] The national regulatory approaches can be differentiated among three main categories, namely statutory regulation, public-private partnership and self-regulation. A decade ago, Christou and Simpson (2007) mapped the landscape of national registries in Europe and the main features of their relationship with the government and the input of government.[21] According to them, the relationship between the registry and the respective government is either qualified as formal or as informal. An example of the former is Denmark, an example of the latter Austria or Germany. The input forms of government vary on a scale from a purely observer status (e.g. Austria or Germany), direct input to management (e.g. Italy), ministerial representation in the board (e.g. France), direct applicable framework legislation (e.g. Denmark), or autonomy based on legislative input (e.g. Sweden). Sometimes, registries are structured as government agency (e.g. Finland) or as fully-state owned company (e.g. Norway). In other words, whereas it is possible to generalize to some degree, it is also important to account for the national specifics in regulatory oversight and influence.

Although this article focuses on country-code domain names and their administration, the system cannot be looked at without at least touching upon gTLDs. Mueller and Badiei (2017) note that whereas "many ccTLD operators are keen to differentiate themselves from their (usually) more commercial 'generic' top-level domain (gTLD) counterparts (...), in fact there is no technical, functional or economic difference between the two."[22] They argue that the "only differences are the legal and political distinctions in the way they are delegated and

socially desirable outcomes when competition cannot be relied upon to achieve them." See Kenneth Train, *Optimal Regulation* (third edn, The MIT Press 1994) 5.

[18] In relation to "Internet management", the European legislator recites the principles of "non-interference, self-management, and self-regulation", see recital 9 of Regulation (EC) No 733/2002 of the European Parliament and of the Council of 22 April 2002 on the implementation of the .eu Top Level Domain, OJ L 113, 30 April 2002, 1–5. See Lee Bygrave, *Internet Governance by Contract* (OUP 2015), 50–84.

[19] Mandate from Internet Assigned Numbers Authority (IANA), which "the overall authority for the IP Addresses, the Domain Names, and many other parameters, used in the Internet." See Lee Bygrave et al., 'The naming game: governance of the Domain Name System' in Lee Bygrave and Jon Bing, *Internet Governance: Infrastructure and Institutions* (OUP 2009). Wolfgang Kleinwaechter, 'From Self-Governance to Public-Private Partnership: The Changing Role of Governments in the Management of the Internet's Core Resources' (2003) Loyola of Los Angeles Law Review, 1103–1126. Emily Weitzenboeck, 'Hybrid net: the regulatory framework of ICANN and the DNS' (2014) 22 International Journal of Law and Information Technology, 49–73.

[20] See *Bygrave* (2015) 78.

[21] See for a comprehensive, but outdated account: *Christou and Simpson* (2007) 12. See also *Bygrave et al.* (2009) 178.

[22] Milton Mueller and Farzaneh Badiei, 'Governing Internet Territory: ICANN, Sovereignty Claims, Property Rights and Country Code Top-Level Domains' (2017) 18 Col. Sci. & Tech. L. Rev., 445.

regulated".[23] From a governance perspective, gTLD registries are directly regulated via ICANN's "contractual web".[24] Given the recent rush into new generic top-level domain names, it is likely that ICANN rules will to a higher degree become a benchmark for the role of domain registries regarding unlawful content. National and European lawmakers as well as national ccTLDs or their industry organisations might look towards these practices and when adjusting their own framework and practices.

3. The liability of intermediaries on the Internet

With the ubiquitous opportunities to spread information on the Internet, both lawful and unlawful content is being distributed. Take-down of unlawful content at source (i.e. server) is undoubtedly most effective, but it is often argued to be ineffective to find the person that made the content available in the first place. Intermediaries, on the other hand, are highly visible middlemen that have the technical possibility, to a varying degree, to inhibit the dissemination of information and thus theoretically halt unlawful content or make its access more difficult. This constitutes the practical appeal to police such content via intermediaries rather than the infringer.[25] In most cases, however, these intermediaries will merely "facilitate or enable the relevant primary conduct by the contemnor."[26] This is also the case for domain registries, who, as described above, neither provide the content nor contribute to its provision as such. Rather, a DNS-registry is merely "assisting the registrant to register a domain name later used tortiously."[27] Furthermore, domain registries are not capable of removing the content and bring an alleged infringement to end but merely take action regarding the domain name, which is not the issue. This is, however, as Truyens and Van Eecke (2016) argue, not different from the role of other intermediaries in the early 2000s.[28] A far-reaching liability might, however, have chilling effects, for example, when the introduction of content control systems is so expensive that the service is not offered in the first place and additionally restricts freedom of information and speech. The liability question is thus not only one in the arena of commercial interests, but also brings up underlying questions of information freedom, freedom of expression, the role of private organisations in the enforcement of rights and thus fundamental rights.

There are two main ways to differentiate the liability of intermediaries: firstly, one can look at the specific content form (e.g. copyright, defamation or free speech). In this vein, a discussion of responsibility is not content-neutral but rather looks at whether the alleged infringement finds its basis in criminal or in private law. A second approach is to differentiate between the different intermediaries or their respective functions (i.e. Internet access provider, hosting etc.). In light of the goal of this article, namely to cast light on tendencies for specific intermediaries and topics, it seems natural to focus on intermediaries rather than content.

[23] *Mueller and Badiei* (2017) 446.
[24] ICANN also maintains contractual links to some ccTLD registries, see *Bygrave* (2015) 77–80.
[25] See also recital 59 InfoSoc Directive: "(...) In many cases such intermediaries are best placed to bring such infringing activities to an end".
[26] *Riordan* (2016) 375.
[27] *Riordan* (2016) 203.
[28] *Truyens and Van Eecke* (2016) 343.

a) Domain registries as intermediaries and information society services

Whereas notably not defined in the European primary or secondary legal framework, intermediaries are addressed in secondary EU legislation, for example in Article 8(3) of Directive 2001/29/EC (InfoSoc)[29] and Article 11 of Directive 2004/48/EC (IPRED)[30], laying out civil remedies for infringements of IPRs in form of injunctions. Generally, the intermediary notion appears to be used fairly broad and was, for example, in case C-557/07 *LSG v Tele2* applied to Internet access providers by the Court of Justice.[31] Moving away from the EU law-specific legal notion towards a more conceptual genus of "intermediary", there is little reason to assume that domain registries would not be considered intermediaries, when looking at the definition provided by OECD.[32] Domain name registries, too, are a party in process of the access to content between the Internet user at the one end and the content that is being accessed on the other. Yet, it is important to acknowledge that domain registries are different to other intermediaries: when an Internet user enters a domain name, the registry merely returns the IP-address of the server but is not forwarding the content as such. Even more, registries do not fit the view of more "active" intermediaries, which for example enhance material provided by users. Rather, as seen above, domain registries provide a function that helps "navigating", somewhat akin to a telephone book or traditional linking, and a "registry" function somewhat akin to a property or company register. Given these intermediary-like properties and in the absence of a more suitable terminology, I suggest looking at domain registries as "intermediaries" in a descriptive and not EU law-specific reading. It is also important to note that the "intermediary" notion in the context of this article is not decisive regarding domain registries' liability or liability exemption.[33]

A second notion in the European framework refers to "information society services".[34] Such service is defined as autonomous concept in Directive 2015/1535/EU (Technical Standards) as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services" in Article 1(1) lit. b. Domain registries and their services seem at first glance to fall within the scope of such service.[35] Neither is the provision of DNS-services contained in the indicative list of excluded services in Annex

[29] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, OJ L 167, 22 June 2001, 10–19.
[30] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 195/16 2 June 2014, 16–25.
[31] *LSG v Tele2*, C-557/07, ECLI:EU:C:2009:107. The court held that "[a]ccess providers which merely provide users with Internet access, without offering other services such as email, FTP or file-sharing services or exercising any control, whether *de iure* or *de facto*, over the services which users make use of, must be regarded as 'intermediaries' within the meaning of Article 8(3) of Directive 2001/29." In *Telekabel Wien* C-314/12, ECLI:EU:C:2014:192, the Court of Justice refined that whereas a service must be capable of being used in order to infringe IPRs, it is not necessary that it maintain a specific relationship with the infringer, paras. 32 and 35.
[32] See above. The OECD's definition is somewhat imprecise. In fact, the OECD report mentions 'domain name registrars' as intermediaries, see *OECD* (2010) 10. See also *Bridy* (2017) 2.
[33] Neither the E-Commerce Directive nor its U.S.-American counterparts operate with the "intermediary" notion. The only reference is in the heading of section 4 on "Liability of *intermediary* service providers" (emphasis added).
[34] The E-Commerce Directive addresses "information society services", see Article 1(1) and (2). Interestingly, the NIS Directive addresses "digital services" and further defines online market places, online search engines and could computing services, recital 55 NIS Directive.
[35] See similar *Truyens and Van Eecke* (2016) 334.

I. Riordan (2016) argues that the "information society service concept" is "a slightly narrower category than the field of internet services at large, but it remains a very broad *genus*, and may be wider than the class of persons who can be said to act as internet intermediaries."[36] He further argues that "a purposive construction suggests that 'information society service' should be construed broadly."[37]

Truyens and Van Eecke (2016), however, point to the fact that "DNS-queries can almost always be submitted free of charge", which could give rise to questions as to whether domain registries provide a service "normally provided for remuneration".[38] They argue that the issue would not be relevant for registrars "as they are almost always commercial entities with profit-making goals"[39] but oversee that neither registrars charge the user of DNS-queries; thus the question is equally relevant for both registries and registrars. Indeed, the non-profit criteria and the important public function of domain registries has been underlined in several of the sparse national cases.[40] However, as pointed out in preparatory works to the E-Commerce Directive, also free services can qualify as "normally provided for remuneration", because in accordance with case law by the Court of Justice, there exists no requirement that the service is paid for by those for whom it is performed.[41] In the case of domain registries, registrants of a domain name pay a fee to the registrar or registry, for the DNS-services to be provided. Regularly these fees cover the operational costs and, whereas not tested by the European courts, it seems reasonable to assume that both registrars and registries would qualify as information society services within the meaning of the Technical Standards Directive.

b) Liability of domain registries for website content

It is clear that DNS services, or registry services more specifically, are not directly used to infringe rights, when looking at the *content* of websites vis-a-vis the *domain name* as such. At best, registry services are used to make infringements easier to access for users, somewhat akin to search engines or other platforms that link to content. Before looking at potential liability privileges, it is necessary to determine the existence and conditions of a contributory or indirect liability of domain registries for infringements by their registrants. Other than limitations on the liability of certain Internet intermediaries, the question whether domain registries have a contributory (criminal or civil) liability for content to which domain names link, is not harmonized by EU law and up to the national legal regime.[42] The question has neither been subject to EU proceedings and there exists only little national case law. Thus, I will in the following rely on evidence from national case law and

[36] *Riordan* (2016) 387.
[37] *Riordan* (2016) 388.
[38] *Truyens and Van Eecke* (2016) 335.
[39] *Truyens and Van Eecke* (2016) 335.
[40] See below.
[41] European Parliament, Committee on Legal Affairs and Citizens' Rights, 'Report on the proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market' (COM(98)0586, 23 April 1999) making reference to *Bond van Adverteerders* Case 352/85, ECR 1988, 2085, point 16. See also *Mc Fadden*, C-484/14, ECLI:EU:C:2016:689, para 43.
[42] See also Article 11 of IPRED Directive and Article 8(3) InfoSoc Directive.

general law principles rather than engage in a comparative analysis of the liability regimes of different Member States, in order to sketch some broader tendencies.

aa) United Kingdom

In October 2013, Cartier International AG brought a test case against the domain registry Nominet seeking an order from the High Court of Justice to "de-tag and lock" 12 .uk domain names, which were allegedly used for the sale of counterfeit watches.[43] The respective domain names made no reference to the trademark but contained generic terms (e.g. mywatchesonline.co.uk). No final judgment in the test action is publicly available.[44] Yet, the case displays the rightholders' interest in testing the liability of the domain registry.

bb) Belgium

In Belgium, the local Anti-Piracy Federation (BAF) brought a case against the local registry, DNS Belgium, involving website content that infringed copyright of Nintendo. In its decision from 9 August 2013, the Court of First Instance in Brussels held that the domain registry is to be considered an intermediary within the meaning of the Belgian Copyright Act.[45] The court confirmed that the registry has neither the competence nor an obligation to perform a legal assessment of content stored on servers to which the domain name links. Notably, the court found that an obligation for the registry to act upon notices by BAF would result in DNS Belgium having to perform a close examination of the case, which would not be proportionate considering DNS Belgium's freedom of business. Rather, the registry's obligation to act was deemed to exist only if an infringement is determined by a court ruling.[46] Finally, the court recalled that DNS Belgium in effect does not have to fear liability from domain name registrants.[47]

dd) Germany

The German Federal Court of Justice (Bundesgerichtshof (BGH)) has in several decisions established that the German ccTLD-registry, DENIC, is not obliged to control whether a domain name *as such* infringes name rights of third parties and held that the registry cannot be held liable as interferer (according to the German concept of "Störerhaftung"[48]).[49]

---

[43] *Cartier International AG v Nominet UK*, Claim No HC13 B04781 (4 November 2013, High Court of Justice, Chancery Division). The case is more known for its parallel main proceedings regarding trademark and blocking by Internet access service providers.

[44] See also *Riordan* (2016) 204.

[45] *BAF v DNS.be*, Rb. Brussel (Nl.), 9 August 2013, 2012/12072/A.

[46] In other words, the assessment of whether an infringement is evident must be assessed by a court, para 9.4 of the judgment.

[47] Alain Strowel and Eric Daems, 'Belgien (.be)', in Torsten Bettinger (ed), *Handbuch des Domainrechts* (Carl Heymanns, 2nd edn, 2017), 518.

[48] "Störerhaftung", literally interferer or disturber liability, is a long established German liability concept in general civil law (§§ 823, 1004 Bürgerliches Gesetzbuch (BGB)), copyright law, and administrative and police law. According to the German case law, an interferer is a party that, without being perpetrator or participant, willfully makes a sufficiently causal contribution to the direct infringement of a protected right.

[49] *ambiente.de*, Judgment of BGH, 17 May 2001, I ZR 251/99; *kurt-biedenkopf.de*, Judgment of BGH, 19 February, I ZR 82/01; *regierung-oberfranken.de*, Judgment of BGH, 27 October 2011, I ZR 131/10. In Germany, when looking at the proportionality of investigation duties on intermediaries, different aspects are considered by the Courts such as interest of the general public in smooth operations, operation in the public interest and nonprofit.

Such a liability is only conceivable, if the registry had been made aware of a "blatant, and for its employees easily identifiable infringement of rights referring to the name" and rejects to act upon such notice.[50]

The first attempt to hold the German registry liable for content dates back to 2001 and involved proceedings for a preliminary injunction in the case *r-e-y.de*.[51] In the civil case, the Regional Court of Wiesbaden denied DENIC's liability for infringing website content. The court cited as a requirement for interferer liability that the registry can prevent the infringement. This was denied in the case towards the background that the registry merely can delete the domain name as such, whereas the content remains accessible via its IP-address. Additionally, the court argued that the website could be easily made available under a different TLD. The court also expressly states that difficulties in the enforcement against the infringer do not play into the liability claim against the registry. Later, the relation of the German registry to content of websites was also subject to two cases under administrative law. In one case, dating back to 2008, the local authority had ordered DENIC to disconnect the domain name of an unlicensed gambling website.[52] After a second order, the government argued that DENIC participated in the provision of the unlicensed gambling website. DENIC called upon the Administrative Court of Düsseldorf, which held that the registry was not liable as interferer even if aware of the infringements on the website to which the .de-domain name re-routed.

Intriguingly, there are several more recent lower instance cases, where registrars were held liable as interferers. The first case, *h33t.com*, dates back to 2013, when Universal Music brought proceedings at the Regional Court of Saarbrücken for a preliminary injunction against a German registrar, whose registrant offered one of the at the time largest torrent trackers under a .com-domain.[53] The Regional Court granted the injunction against the registrar, which was upheld in appeal by the Higher Regional Court of Saarbrücken.[54] The court confirmed interferer liability, arguing that the registrar had via registering the domain name contributed in "adequate causative" ways so that the registrant and visitors of the domain infringe copyright by means of the domain, even when the content continues to be available directly via the IP-address. Furthermore, it was deemed that the IP-address was "considerably simpler and easier accessible" via the domain name.[55] In line with previous case law on names *as such*, the court denied a general duty to investigate or monitor content on domain names, but found the registrar liable for not acting upon notice of alleged infringements,

[50] *regierung-oberfranken.de*, para 26.
[51] *r-e-y.de*, Judgment of LG Wiesbaden, 13 June 2001, 10 O 116/01, ECLI:DE:LGWIESB:2001:0613.10O116.01.0A
[52] Judgment of VG Düsseldorf, 29 November 2011, 27 K 458/10, ECLI:DE:VGD:2011:1129.27K458.10.00. See also below.
[53] *h33t.com*, Judgment of LG Saarbrücken, 15 January 2014, O 82/13, ECLI:DE:LGSAARB:2014:0115.7O82.13.0A, GRUR-RS 2014, 02993. The registrant had not responded to a take-down notice by the rightholder regarding a link to the Robin Thicke album Blurred Lines.
[54] *h33t.com*, Judgment of OLG Saarbrücken, 22 October 2014, 1 U 25/14, ECLI:DE:OLGSL:2014:1022.1U25.14.0A, MMR 2015, 120. The decision h33t.com has received media attention and been partly welcomed by practitioners as and "ground-breaking", see Bernd Nordemann, MMR 2014, 407 (note).
[55] *h33t.com*, Judgment of OLG Saarbrücken, 22 October 2014, 1 U 25/14, ECLI:DE:OLGSL:2014:1022.1U25.14.0A, MMR 2015, 121.

which were "blatant" and could be ascertained without further ado. In 2014 and 2015, several other German lower court decisions also confirmed interferer liability of registrars in cases of violations of personality rights and by transferring the liability of hosting providers to registrants.[56] In yet another decision from 2015, the LG Frankfurt am Main convincingly rejected the general transfer of the principles of hosting providers to registrars.[57] As recently as December 2017, the LG Köln confirmed the interferer liability of a registrar for the content accessible via several Pirate Bay-related domain names, even in the case where the registrar does not connect the domain name but merely forwards the registrants application to the respective registry.[58] Thus, it is apparent that the threshold for the secondary liability of registrars is much lower than for the national ccTLD registry. The argumentation of the courts, however, is puzzling compared to previous findings of (another) court regarding the ccTLD registry which argued the exact opposite.[59]

ee) Sweden

Also the Swedish ccTLD registry, Internetstiftelsen (IIS), was subject to proceedings regarding content involving the domain names *thepiratebay.se* and *piratebay.se*. The case dates back to 2013, when the Swedish anti-piracy group Rights Alliance filed a motion to have the domain seized and a complaint against IIS. The registry, on the other hand, argued that it had no obligation to act but rather an obligation not to act without the direct instruction from e.g. a law-upholding authority. In the course of the proceedings, the prosecutor argued that as controller of those domains, IIS should also be held liable for copyright infringement.

In May 2015, the Stockholm District Court ruled that the respective domain names must be seized. Regarding forfeiture of the domain names and the role of the registry, the court reiterated that liability for complicity ("medverkansansvaret") in Swedish law is fairly extensive and already an insignificant furtherance may suffice.[60] It argued that the registry acted with intent insofar it had decided not to act upon the respective domain names.[61] When examining limitations to liability for complicity, however, the court found that unlike an Internet access service provider that provides services for commercial gains, the national ccTLD registry acted based on other considerations pointing towards the domain name administration assignment as important public function, which "does not entail pronouncing judgement on what could be considered unlawful or not in an individual case".[62] Thus, the

[56] Court order of KG Berlin, 10 July 2014, 10 W 142/13, ECLI:DE:KG:2014:0710.10W142.13.0A, NJW 2015, 795. Also Judgment of LG Köln, 13 May 2015, 08 O 11/15, ECLI:DE:LGK:2015:0513.28O11.15.00, MMR 2015, 523.
[57] Court order of LG Frankfurt am Main, 5 August 2015, 2-03 O 306/15, ECLI:DE:LGFFM:2015:0805.2.03O306.15.0A. The court argued that, whereas potentially not directly applicable, the valuations of the liability privileges also apply to injunctive relief in relation to reasonable control duty by the intermediary.
[58] Judgment of LG Köln, 5 December 2017, 14 O 125/16. The case has been appealed. Notably, the court found the liability privileges of the German implementation of the E-Commerce Directive do not apply to injunctive relief, 21.
[59] See above *r-e-y.de*, Judgment of LG Wiesbaden, 13 June 2001, 10 O 116/01, ECLI:DE:LGWIESB:2001:0613.10O116.01.0A.
[60] Judgment of Stockholm District Court, 19 May 2015, B 6463-13, 19.
[61] Ibid at 18.
[62] Ibid at 21.

court denied a liability for complicity of the registry. This reasoning was also upheld in the 2016 appeal to the Swedish Svea Court of Appeal.[63] In its judgment, the Court of Appeal noted that whereas the registry in accordance with the national top-level domain Act has the responsibility of maintaining its register and under its terms and conditions even retained the right to de-register or deactivate a domain name if the domain name itself or its use conflicts with law or statute, it "clearly" only has an administrative role in the domain name system under the supervision of a Swedish government agency.[64]

ff) Tendencies in registry liability

This article does not aim at a thorough analysis of national liability regimes, but rather relies on sketching some overall tendencies. Even if case law on secondary liability of domain registries is scarce, there seems to be an increasing tendency, especially from rightholders, to turn towards this type of intermediary. Strikingly, the majority of the available cases concern civil liability for the infringement of IP rights.

The sparse national case law appears to share some commonalities, namely a focus on "public service" and administrative functions of national ccTLD registries. In some cases, the non-profit nature of domain registries seems to weigh in additionally. It becomes apparent, for example, that the German lower courts' jurisprudence regarding the domain registry DENIC is fairly consistent in denying secondary liability for website content. Additionally, based on the German Federal Court of Justice's findings regarding the legality of domain names (in respect to infringements of name rights), it would seem *a maiore ad minus* inconsistent to hold the registry liable for content, which is much further away from the registry than the domain name as such. Correspondingly, if there is no obligation to monitor the domain name as such, it would seem illogical to require the monitoring of its use, left aside the compatibility with other rules.

From the jurisprudence, it seems extremely unlikely that registries have any obligation to act on their own initiative.[65] A different question is, whether domain registries could become liable if they refrain from acting after being notified of an alleged infringement (i.e. without a court ruling). The Belgian and German examples could indicate that in the most blatant, obvious cases of illegal uses, secondary liability is conceivable, yet with the caveat that the existing German jurisprudence regards domain names *as such*. The Swedish decision, on the other hand, seems to restrict these instances to the direct instruction from e.g. a law-upholding authority. Registrars, on the other hand, at least in the (incoherent) German case law, appear to be less privileged. It also apparent that the nature and concept of domain registries or registrars is not understood in the same way by all lower courts.

[63] Judgment of Svea Court of Appeal, 12 May 2016, B 5280-15.

[64] Regarding forfeiture, the Court of Appeal concluded that the registry does not have "such property rights in the form of the right of disposition over a registered domain name that would constitute a right of ownership as required by the forfeiture legislation", Judgment of Svea Court of Appeal, 12 May 2016, B 5280-15, 13.

[65] In Denmark, for example, the general administration principles in the Administration of Justice Act enable the courts to require telecommunication providers to block content. The duty to block arises already when content is found evidently unlawful.

The courts' argumentation for a direct transfer of the liability principles of hosting providers to registrars is unconvincing and appears unlikely to be transferred to ccTLD registries, given their special function for the public. Yet, it cannot be precluded that there will be future attempts to hold registries liable – beyond injunctions – for content, similar to for example Internet access service providers.[66] In light of the demanding but varying national conditions for secondary liability "derived from miscellaneous doctrines of tort law, such as the doctrines of joint tortfeasance, authorization, inducement, common design, contributory liability, vicarious liability or extra-contractual liability"[67], it can neither be precluded that domain registries will be held liable. Additionally, some Member States have chosen to address secondary or third-party liability of intermediaries, for example online platforms, in domestic secondary legislation;[68] a trend that might not stop at this type of intermediary. Additionally, recent developments in the CJEU case law on Internet access service providers might also have implications for domain registries and their liability.[69] Thus, it is worth considering, whether domain registries can benefit from liability privileges of the E-Commerce Directive.

4. Liability privileges for domain registries

Many jurisdictions have addressed the liability of intermediaries by enacting exemptions from secondary liability for their users' content, often in e-commerce or copyright laws.[70] In Europe, for the last 17 years, the general legal framework for intermediary liability exceptions of information society services is contained in the E-Commerce Directive. Despite its age, the European Commission concluded in 2016 that the existing regime is fit for purpose, but that regulatory action is needed to tackle the proliferation of illegal content online.[71] The European Parliament, on the other hand, calls for a clarification of the liability of intermediaries in 13 points of its resolution from 2017.[72]

[66] See also the debate in the previous literature on the applicability of the liability exemptions, which necessarily prerequisites the liability of domain registries in *Truyens and Van Eecke* (2016).

[67] Giancarlo F. Frosio, 'From horizontal to vertical: an intermediary liability earthquake in Europe' (2017) 12 Journal of Intellectual Property Law and Practice, 570.

[68] A recent example for domestic regulation on third party liability for online platforms comes from Germany. In September 2017, the Network Enforcement Act (Act to Improve Enforcement of the Law in Social Networks) introduces the liability of social media providers such as Facebook or Twitter for third party content.

[69] In the relatively recent decision in *UPC Telekabel Wien*, C-314/12, ECLI:EU:C:2014:192, the Austrian Supreme Court referred to the European Court of Justice a question regarding the unauthorised making available of films via the website kino.to and the role of Internet access service providers. The court held that the Internet access service provider must be seen as intermediary whose services are used to infringe a copyright or related right within the meaning of Article 8(3) Directive 2001/29/EC and that broad blocking injunctions are compatible with EU law (see also footnote 31 above). The judgment is to be seen against its distinct Austrian legal background, but still provides difficulties in its relation to the court's earlier findings in *Scarlet v SABAM*, C-70/10, ECLI:EU:C:2011:771 and *SABAM v Netlog*, C-360/10, ECLI:EU:C:2012:85. See Tatiana-Eleni Synodinou, 'Intermediaries' liability for online copyright infringement in the EU: Evolutions and confusions' (2015) 31 Computer Law & Security Review 57–67.

[70] In the U.S. e.g. Section 230 of the Communications Decency Act (CDA) of 1996, Section 512 of Digital Millennium Copyright Act (DMCA) of 1998.

[71] European Commission, 'Online Platforms and the Digital Single Market, Opportunities and Challenges for Europe' (Communication), COM(2016) 288 final.

[72] European Parliament, 'Resolution of 15 June 2017 on online platforms and the digital single market' (2016/2276(INI)), points 29–41.

The E-Commerce Directive offers a safe harbor for criminal liability, damages, and pecuniary liability, whereas injunctions are allowed. Recital 42 of the Directive stipulates that the exemptions only cover situations where the activity of the service provider is "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." *Prima facie* domain registries fulfill these criteria, too. Registries are, however, not directly addressed in the secondary liability regime of the Directive and there is no evidence that the European lawmaker had the DNS in mind when drafting and adopting the framework in the late 1990s. In fact, the only place where the E-Commerce Directive mentions the DNS is in Article 2 lit. f, where it excludes domain names from the scope of commercial information. Truyens and Van Eecke (2016) also find it from a structural point of view questionable, to what extent the content-related regime of the Directive indeed is applicable to domain registries, which operate at an infrastructure level.[73] Thus, in a narrow reading, the applicability of the Directive could be negated. On the other hand, neither are other intermediaries addressed *expressis verbis* in the Directive. Rather, the Directive works with the information society services notion and a functional horizontal approach covering various industry verticals and any kind of illegal content. Additionally, national courts have noted that the evaluations of the liability regime ought to be consulted even if the registry does not fall within the scope of the national e-commerce legislation.[74] Given this *lacuna*, the question is whether the regime of the Directive can be applied to domain registries or where to place the administrators of the DNS in the regime. In the following I therefore differentiate between different categories of intermediaries and test to what extent domain registries fit.

a) Mere conduit (Internet access service providers)

Article 12(1) E-Commerce Directive provides a safe harbor for information society service providers "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" under certain cumulative conditions namely: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission. Internet access service providers are the prototype provided with the liability privilege of Article 12. The question is whether Article 12(1) also encompasses domain registries and their activities.

The first "mere conduit" scenario of Article 12(1) relates to the transmission of information provided by a recipient of the service in a communication network. As seen above, domain registries provide name server and registry services for the respective top-level domain. The name servers of the domain registry provide the assignment of domain names to the IP addresses of the server. Additionally, the registry maintains a database over domain and contact information in form of a WHOIS-database. German courts argued that registries thus, in a broad sense, provide access to the use of information provided by third parties on a server by assigning domain names to IP addresses.[75] WHOIS-data, on the other hand,

[73] See *Truyens and Van Eecke* (2016), 337.
[74] Judgment of VG Düsseldorf, 29 November 2011, 27 K 458/10, para 33.
[75] Ibid, para 37.

which is stored at the registry, has no relation to the content in question but rather is neutral in relation to the respective infringement.[76] Similarly, Truyens and Van Eecke argue that "authoritative DNS-servers (...) indeed transmit information provided by a recipient because they distribute the domain name (...) throughout the DNS-system, to all non-authoritative DNS-servers, who then distribute this information to all users who submit relevant DNS-queries."[77] Bettinger (2015), on the other hand, argues in the context of domain name specific infringements that it is indisputable that the liability privileges of the E-Commerce Directive (or rather its German implementation) exclusively regard the conduit or storage of information but not the purely technical activity of resolving domain names to IP addresses.[78]

A second line of thought is whether the provision of DNS-services by domain registries qualifies as the "provision of access to a communications network", the second scenario covered by Article 12(1). Riordan (2017), for example, evaluates that DNS intermediaries provide access to a communication network "namely access to the hosts described by the answer to a DNS query."[79] The DNS constitutes a fundamental part of the underlying technology of the Internet as has been acknowledged by the judiciary in the Swedish *Pirate Bay* case.[80] Also, the European lawmaker in regulating the *.eu* ccTLD underlined that TLDs "are an essential element of the global interoperability of the World Wide Web".[81] Additionally, TLD name registries as well as DNS service providers (along with Internet exchange points) qualify as operators of essential services of the digital infrastructure according to Article 4 nr. 4 in connection with Annex II of the NIS-Directive. These two examples need to be seen in their distinct legislative context though and it is questionable whether their valuations can inform the scope of Article 12. More specifically, Truyens and Van Eecke (2016) add that "if a DNS registrar's servers are unavailable, all the websites and email systems of customers who registered domain names with this registrar will appear disconnected from the Internet."[82] Interestingly, regarding domain registrars, a German court points towards the potential difference to domain registries, in the fact that registrars regularly also provide hosting services and thus are in a direct contractual relation to the registrant in respect of content.[83]

It is apparent that the functions performed by registries are difficult to reconcile with the direct wording of the provision. The *raison d'être* of Article 12 is a liability exemption for network operators which provide the technical facilities for transmission but have no control over the data flowing through their network.[84] Against this background, it seems reasonable to argue that domain registries qualify for the exemption under a teleological interpretation

[76] Ibid, para 39.
[77] *Truyens and Van Eecke* (2016), 335.
[78] Torsten Bettinger, 'Germany ('.de')', in *Bettinger* (2015) 438.
[79] *Riordan* (2016) 396.
[80] See above.
[81] See recital 3 of Regulation (EC) 733/2002. Note, however, that the Regulation is without prejudice to national ccTLDs, see Article 1(2).
[82] *Truyens and Van Eecke* (2016) 335.
[83] Judgment of VG Düsseldorf, 29 November 2011, 27 K 458/10, para 39.
[84] See also recital 42 E-Commerce Directive.

of the norm.[85] There is no historical evidence that the legislator had a conflicting evaluation. Rather, it seems likely that the role of the DNS in content-related debates was simply off the lawmakers' radar. Systematically too, it would seem inconsistent if the framework only was to harmonize the liability of services that are close to the content. If registries, on the other side, were not covered by Article 12, they would effectively have a more extensive liability than Internet access service providers. Considering that the intermediary-like functions of registries are even farther away from content than other services addressed in the E-Commerce Directive, this is a result that hardly can have been the intention of the lawmaker. Additionally, such a teleological reading also finds support in case law. Several German courts argued that even if the German registry DENIC would not be covered by the implemented liability rules of the E-Commerce Directive, its underlying evaluations are to be consulted.[86] Thus, it seems convincing that domain registries would be covered by the liability exemption in Article 12 in a teleological interpretation.[87] Consequently, registries would be even exempt from liability when knowing of content-related infringements.[88]

b) Hosting (hosting platforms)

Online storage space providers, or hosting providers, are a second group of intermediaries traditionally addressed in the quest for content take-downs. The liability exemption for these hosting providers in Article 14 of the E-Commerce Directive constitutes one of the more controversial provisions of the Directive.[89] Hosting providers can benefit from the liability exemption according to Article 14 (1) lit. a and b on the condition that "(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information."

One key question is whether the role of the hosting provider qualifies as active. In its decision in *L'Oréal v eBay* from 2011, the CJEU stated that:

> "(…) the mere fact that the operator of an online marketplace stores offers for sale on its server, sets the terms of its service, is remunerated for that service and provides general information to its customers cannot have the effect of denying it the exemptions from liability provided for [Article 14 of the E-Commerce Directive]"[90] but:

[85] Whether this is based on their quality as providers of access to a communications network or as providers that consist of the transmission of information provided by a recipient of the service in a communication network can be left open.

[86] See Judgment of VG Düsseldorf, 29 November 2011, 27 K 458/10, para 33 and Judgment of OLG Saarbrücken, 22 October 2014, 1 U 25/14, MMR 2015, 129. In an earlier decision related to domain names *as such*, the OLG Frankfurt denied the direct as well as the analogue application of the German telecommunications law on the German registry DENIC, see Judgment of OLG Frankfurt, 14 September 1999, 11 U Kart 59/98.

[87] See similar *Riordan* (2016) 396 f.

[88] See also *Mc Fadden*, C-484/14, ECLI:EU:C:2016:689, para 59.

[89] See e.g. Aleksandra Kuczerawy, 'Intermediary liability & freedom of expression: Recent developments in the EU notice & action initiative' (2015) 31 Computer Law & Security Review 46–56.

[90] *L'Oréal v eBay*, C-324/09, ECLI:EU:C:2011:474, para 115. See also *Google France*, C-236/08, ECLI:EU:C:2010:159, paras 114 and 120, and Recital 42 of the E-Commerce Directive.

> "[w]here, by contrast, the [online platform] has provided assistance which entails, in particular optimising the presentation of the offers for sale in question or promoting those offers (…)"[91]

Truyens and Van Eecke (2016) argue that "[f]ollowing the position of the CJEU, DNS-services may then also qualify as protected hosting services in a forward-looking interpretation" of the Directive.[92] As a consequence, registries would be exempt from liability only if they act immediately from notice of infringing content.[93] Interestingly, in one German lower court case, the court held that the principles of liability of hosting providers are to be transferred to domain registrars.[94] Here, however, one can at least theoretically argue that registrars provide other services in addition to their DNS-services, such as hosting which might invoke Article 14. In another German case, a German court clarified that the national registry, DENIC, does not constitute a hosting service.[95] Already from the outset, however, it appears far-fetched to reflect on the applicability of Article 14 to domain registries; after all, domain registries do not host the content of the website. The stored content, namely DNS information and WHOIS-data on the registrant, is usually not itself illegal. Against this background, it appears implausible to subsume registries under the hosting exemption.

Yet another consideration in this context is whether several exemptions can be evoked for the same situation. Here it seems reasonable to once again differentiate between function and intermediary. It also seems to run counter to the Directive's regime that one activity can evoke several exemptions. Against this background it is apparent that one technical function should only trigger one exemption. At the same time, an intermediary might well perform several functions and thus invoke several liability exemptions (think for example of Google which operates as domain registrar but also offers various hosting services).

6. Discussion and concluding remarks

In a resolution of May 1998, the European Parliament called for a coordinated approach and stressed "the importance of a simple, minimalist and predictable legal framework for electronic commerce."[96] Twenty years later, it seems that the endeavour to create this clarity has failed. Domain registries have been on the fringes of content-related liability debates but against the background of the ongoing search for relief for traditional enforcement mechanisms in the online world, they are likely to continue to become a more relevant player in the intermediary-game in the future; a trend that is indicated by the sparse but increasing national case law on domain registries and registrars.

---

[91] *L'Oréal v eBay*, para 116.

[92] *Truyens and Van Eecke* (2016) 337. See para 110 of *L'Oréal v eBay*, where eBay qualified as hosting provider because "it holds in its server's memory data supplied by its customers," and "that storage operation is carried out by eBay each time a customer opens a selling account with it and provides it with data concerning its offers for sale"

[93] See e.g. *Mc Fadden*, para 58.

[94] Judgment of LG Köln, 13 May 2015, 08 O 11/15, MMR 2015, 523 with comment by Thomas Hoeren.

[95] Judgment of VG Düsseldorf, 29 November 2011, 27 K 458/10, para 37.

[96] Resolution on the communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on a European Initiative in Electronic Commerce (COM(97)0157 C4-0297/97), point 11.

This article has shown that the E-Commerce Directive's liability regime might indeed embrace domain registries in a teleological retro-fitting fashion. Against the background of recent case law regarding other intermediaries (e.g. *UPC Telekabel Wien* and others) and the European Commission's recent proposals[97], however, it appears that the intermediaries' safe harbor might be smaller than it looks. A recent policy briefing commissioned by the European ccTLDs umbrella organization, the Council of European National Top-Level Domain Registries (CENTR), acknowledges this changing context.[98] As noted throughout this article, there exist a variety of functional differences between domain registries and other intermediaries such as Internet access service or hosting providers. Functionally, the services of registries somewhat resemble linking rather than other intermediary functions. In a copyright context, the Court of Justice has established a sophisticated stance on linking to illegal content in several recent decisions.[99] Thus, also taking a careful look over the fence might be a worthwhile endeavour. Yet, some shifts in other intermediaries' role could reflect on domain registries. Given these trends, one can ask whether domain registries still can use their infrastructure-rationale to justify refraining from being involved in the fight against unlawful content. It cannot be repudiated that these shifts also lead to a changing landscape for the DNS, whether by direct intervention via the legislators, judiciary or industry self-regulation. Domain registries have come late to the party of intermediary content liability discussions and might be on the verge of de facto accepting a more proactive role in the takedown of content online, potentially a slippery slope.[100]

The underlying question it boils down to, is whether and, if so, to what extent domain registries have an active role in enforcing content on the Internet. On a first glance, the DNS-based actions appear to be an easy way to make unlawful content inaccessible or enforce rights on the Internet. From a legal as well as practical point of view, it is crucial to reflect whether the DNS, without looking at its merits, is a suitable tool to block content in the first place. Given its function as purely turning addresses into "human-friendly" terms, it is important to recall that domain names are not essential for making a website accessible.[101] As one German court puts it, a website is accessed not via the domain name, but via the IP address that is associated with the domain name.[102] Thus, whereas access is being rendered more difficult by removing a domain name, it is still possible to access the content via the underlying IP address, making the removal of a domain name a somewhat toothless tiger.[103]

---

[97] See e.g. Article 13 of European Commission, Proposal for a Directive on copyright in the Digital Single Market, COM(2016) 593 final.

[98] Political Intelligence, 'A New Role of ccTLDs in the EU Regulatory Landscape' (Commissioned by CENTR (Council of European National Top-Level Domain Registries), September 2017), 2.

[99] See notably *GS Media*, C-160/15, ECLI:EU:C:2016:644 as well as *Bestwater*, C-348/13, ECLI:EU:C:2014:2315 and *Svensson*, C-466/12, ECLI:EU:C:2014:76. See also related search engine de-indexing, *Google Spain*, C-131/12, ECLI:EU:C:2014:317.

[100] Maurice Schellekens, 'Liability of Internet Intermediaries: A Slippery Slope' (2011) 8 SCRIPTed, 154–174.

[101] See *Bygrave et al.* (2009) 148.

[102] See e.g. Judgment of LG Wiesbaden, 18 October 2013, LI:DE:LGWIESB:2013:1018.1O159.13.0A, Az. 1 O 159/13, para 37.

[103] That said, it is apparent that domain names play a crucial role in the access to websites. In a different context regarding search results the Court of Justice held for example that the "activity of search engines plays a decisive role in the overall dissemination of those data in that it renders the latter accessible to any internet user making

At the same time, DNS-based remedy is appealing as the respective domain name is disabled globally.[104] The removal of a domain name is a far-reaching measure, too: whereas the content is not taken off the Internet, still access to the content as a whole, i.e. illegal and legal parts, is rendered more difficult. Also, chilling effects as well as over- or under-removal become societal concerns.[105] Additionally, with the de-connection of a domain name associated e-mail addresses become un-functional. Thus, the balancing of interests to safeguard repercussions on fundamental rights such as the freedom of expression, freedom of information, or the right to conduct business is essential and makes for a most relevant aspect to study further.

Domain registries, it seems, are getting caught in the middle. Considering principles such as the rule of law or legal certainty, registries should not have to determine legal content-related issues. In light of retro-fitted and eroding safe harbor provisions they could be incentivized to take-down domain names. At the same time, registries could also be faced with claims from registrants for wrongful action. Either way, it appears advisable to engage in an educated policy debate in order to ensure a coherent regime for their role going forward. The DNS has existed in its form since the emergence of the Internet. It is, however, also important to keep in mind that technological advancements, notably in connection with decentralization and blockchain-based technology, might alter the functioning of the system as we know it today. What better time to re-visit the very principles of the liability exemption framework?

---

a search on the basis of the data subject's name, including to internet users who otherwise would not have found the web page on which those data are published.", see *Google Spain,* C-131/12, ECLI:EU:C:2014:317, para 36.

[104] It will be rendered even more difficult, once the novel standard for the internet protocol IPv6 (128 bit), is broadly implemented, which is intended to replace IPv4 (32 bit). See also fully qualified domain name in RFC 2181: Clarifications to the DNS Specification (authors: R. Elz and R. Bush) (1997) <https://tools.ietf.org/html/rfc2181> accessed 15 January 2018.

[105] See e.g. Katalin Parti and Luisa Marin, 'Ensuring Freedoms and Protecting Rights in the Governance of the Internet' (2003) Journal of Contemporary European Research, 146. The European Commission in its Communication on 'Tackling Illegal Content Online, Towards an enhanced responsibility of online platforms' from September 2017 (p. 6), tries to address "concerns in relation to removal of *legal* content, sometimes called 'over-removal', which in turn impacts freedom of expression and media pluralism. Adequate safeguards should therefore be foreseen, and adapted to the specific type of illegal content concerned."