INTERNET POLICY REVIEW
Journal on internet regulation

Volume 9 | Issue 1

The regulation of abusive activity and content: a study of registries' terms of service

Sebastian Felix Schwemer
Centre for Information and Innovation Law (CIIR), University of Copenhagen, Denmark, sebastian.felix.schwemer@jur.ku.dk

Published on 31 Jan 2020 | DOI: 10.14763/2020.1.1448

Abstract: This paper studies the role of domain registries in relation to unlawful or unwanted use of a domain name or the underlying website content. It is an empirical and conceptual contribution to the online content regulation debate, with specific focus on European country code top-level (ccTLD) domain name registries. An analysis of the terms of service of 30 European ccTLD registries shows that one third of the registries contain some use-related provision, which corresponds to approximately 47% of registered domains. The analysis also turns towards examples of notice-and-takedown mechanisms, the emergence of proactive screening and the practice of data validation. Based on the analysis, it calls for more clarity and transparency regarding domain registries' role in content- or use-related takedowns.

Keywords: Content regulation, Domain names, Terms of Service (TOS), Takedown, Abuse

Article information

Received: 17 Jul 2019 **Reviewed:** 10 Oct 2019 **Published:** 31 Jan 2020
Licence: Creative Commons Attribution 3.0 Germany
Funding: This article is the result of a research project that has been funded by the Innovation Fund Denmark and the Danish Internet Forum (DIFO).
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/regulation-abusive-activity-content-study-registries-terms-service

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

INTRODUCTION

Policymakers, internet giants and other players look frantically for solutions to the problem: who should enforce unlawful content and behaviour on the internet and under what conditions? Much of this debate focuses on well-bespoke intermediaries like online platforms or internet access service providers.

Domain names act as road signs of the internet with their essential function of resolving names to IP addresses (see Bygrave et al., 2009). Whereas "architecture lies well beneath the level of content (...) [i]nfrastructure design and administration internalize the political and economic values that ultimately influence the extent of online freedom and innovation" (DeNardis, 2012, p. 721). While this part of infrastructure traditionally stayed off the radar in content debates despite "IP addresses [being] at the center of value tensions between law enforcement and intellectual property rights versus access to knowledge and privacy" (DeNardis, 2012, p. 724), this has changed more recently (Schwemer, 2018; Internet & Jurisdiction, 2019a, pp. 159–161). In 2019, for example, the domain name industry association, Council of European National Top-Level Domain Registries (CENTR), issued a report on "Domain name registries and online content" (CENTR, 2019b). At the ICANN66 meeting in Montréal (GAC, 2019) and the Internet Governance Forum (IGF) in Berlin, "abuse"[1] was a prominent topic on the agenda. At the same time, computer scientists and cybersecurity researchers have looked at the role of the domain name system (DNS) and malicious activities (Hao et al., 2013; Vissers et al., 2017; Korczyński et al., 2017; Kidmose et al., 2018).

In this article, I look at the terms of service (ToS) of European ccTLD registries with a view to identify their stance on content- or use-related domain name takedowns: What do the ToS of ccTLDs say on *use* of a domain name and more specifically about *content* on the underlying website?

ToS of domain registries have so far received limited attention. In 2017, Kuerbis, Mehta, and Mueller (2017), for example, empirically looked at the ToS of selected generic top-level domain (gTLD) registrars in relation to morality clauses, which enable the registrar to cancel a domain name for content-related reasons. From a consumer perspective, also in 2017, the Electronic Frontier Foundation (EFF) looked at the question, "Which Internet registries offer the best protection for domain owners?" from a trademark, copyright, overseas speech regulation, and identity theft perspective (Malcolm, Rossi, & Stoltz, 2017).

This article aims at making a contribution to the study of regulating and enforcing "abusive" *activity* or *content* by intermediaries and specifically the role of ccTLD registries. Methodologically, it is based on a comparative analysis of 30 selected ToS of European ccTLD registries governing the bilateral contractual relationship between registry and registrant.[2] Whereas it is also worth further to study the practical application of these ToS, e.g., by a multi-method approach integrating insights from interviews with registries or other data provided by registries, the focus of this contribution is on exploring the contractual room of operations that ccTLD registries reserve in their ToS *vis-à-vis* registrants. ToS serve as a primary legal basis in this relation (see below) and there is a strong point in looking at these ToS based on publicly available information without further interpretation provided by registries, which normally would be inaccessible for registrants in a structured manner. Ultimately, also courts would look at the ToS rather than the practice of that specific registry in their legal assessment, because courts would not be bound by industry practice. In many instances, the registration of a ccTLD name will not be performed by the registrant directly at the registry but rather through a registrar, i.e., a reseller, where additional terms regarding the use of domain names might be applicable. Contractual relations between registrants and registrars, as well as a study of the underlying national legislative frameworks are outside the scope of this analysis. Other sources of domain name takedowns, notably court orders or specific legislation are also outside the scope of this paper.

With this article, I want to contribute to specifying and defining the issue in light of increasingly blurred lines when talking about "takedown", "abuse" or "use" in the field of domain names and use or content on the underlying website. Here, I am only interested in takedowns related to the *use* of a domain name or the content made accessible via a domain name. Issues related to a domain name *as such*, such as in the case of e.g., typosquatting, are a relatively well-studied phenomenon (see e.g., Moore, Clayton, & Anderson, 2009; Bettinger & Waddell, 2015; EUIPO, 2018) and outside the scope of this paper. This article provides an overview on emerging mechanisms that European ccTLDs have employed in relation to use- or content-related domain name takedowns.

INTERNET GOVERNANCE, THE CCTLD LANDSCAPE AND "ABUSE" OF OR ON INFRASTRUCTURE

This article's core subject has its roots in different internet governance dynamics, the first of which concerns the differentiation of country-code top-level domain names (ccTLD) and generic top-level domain names (gTLDs). There are approximately 71 million domain names under the management of 57 CENTR ccTLD registries with an average local market share of 54% (CENTR, 2019). The top 5 EU/EFTA ccTLDs are <.de> (16,2m), <.uk> (12,17m), <.nl> (5,87m), <.eu> (3,66m), and <.fr> (3,4m). This compares to globally 194 million gTLD domain names, whereof 71% are registered under <.com> (CENTR, 2019).

The two systems vary considerably in their institutional and governance setup (Bygrave, 2015, p. 77ff.), while "in fact there is no technical, functional or economic difference (...)" (Mueller & Badiei, 2017, p. 445). Compared to gTLDs, public interest considerations are especially dominant in the ccTLD sphere as Geist (2004, p. 9) notes. ccTLDs have as institutions existed since 1985 (Aguerre, 2010, p. 7) and become "in-country political and economic institutions" (Aguerre, 2010, p. 11; Park, 2008). Whereas the non-profit Internet Corporation for Assigned Names and Numbers (ICANN) "has the authority to make certain policy decision regarding the domain namespace" of gTLDs, which are managed internationally and also subject to the laws of their country of incorporation, ccTLDs are "mainly subject to the national sovereignty of the respective country" (Mahler, 2019, p. 3). The governance of ccTLDs has been described as a system of "non-state, private actors operating within a broader public-private network" (Christou & Simpson, 2007, p. 17) where yet "[g]overnments are deeply involved in domain name administration at the national level" (Geist, 2004, p. 2). Kleinwächter (2003, pp. 1105–1106) explains the "bottom-up development by private stakeholders without any interference from governmental legislation" in the early days with the rapid growth of the internet and notes "[f]ew governments considered the DNS worthy of attention". More recently, DNS providers have appeared on the lawmakers' radar and have been, for example, addressed in the NIS Directive of 2016.[3]

In the online environment, contractual relations, regularly defined by terms of services (ToS), constitute a primary regulatory factor (Belli & Venturini, 2016; Kuerbis, Mehta, & Mueller, 2017), despite often being disregarded by users (in the context of social networking services, see Obar & Oeldorf-Hirsch, 2018). Given their powers, private intermediaries, in some instances, are seen by some as acting akin to governments or as *de facto* regulators (Riordan, 2016, p. 343). For the management of country-code top-level domain names (ccTLDs) there exists a "statutory footing" in primary or secondary legislation in some instances (Bygrave, 2015, p. 78). Often, domain registries, however, have a broad freedom to define the ToS for the granting and use of domain names under their respective top-level domain (TLD). Against the payment of a fee, and on a first come, first served basis, a registrant regularly obtains a right to use the domain name (interestingly, in the French <.fr> zone, a registrant "owns the domain name"). Some registries restrict registration of ccTLD domain names to residents from certain countries (e.g., <.no> and <.it>). The contractual relation between registry and registrant also provides one potential basis for out-of-court takedowns. Thus, in order to understand the regulatory landscape for content- or use-related domain name takedowns it is necessary to focus on the registries' regulation via their ToS.

The notion of "takedown" in relation to a domain name is not unproblematic: technically, administratively and partly legally, a more thorough distinction between blocking, suspension (the technical decoupling from a name server), deletion (registrant is deleted in the WHOIS-database), deactivation, transfer, seizure, etc. of a domain name is necessary. There exists no uniform notion among registries, lawmakers and practitioners. The goal of a domain name-related measure for *content* reasons is typically that the domain name can no longer be used to access a website (DeNardis, 2012, p. 728; Schwemer, 2018, p. 277), even though the content remains accessible via the IP address: this can be achieved by suspending or deleting a domain name, whereas blocking goes beyond that (presuming that there exists a societal interest in domain names being used). For the sake of this article, in any case, all these measures will be understood as takedown.

Despite the fact that it is sometimes seen as a controversial term, "abuse" is becoming an ever more frequently used term in the domain name world, which according to Mahler (2019, p. 252) is to be understood in a broader way than just covering illegal activity. Again, there exists no uniform definition. While, strictly speaking, the ccTLD world is somewhat detached from ICANN policy, ICANN's attempt to define the issue provides a valuable perspective on abuse. Mahler (2019, p. 249) notes that in ICANN's regulatory framework, too, there exists no clear definition of abuse and it can span from undesired activities like sending out spam, which is not necessarily a criminal offence, to copyright infringements, and ultimately the commission of cybercrime.[4] In 2010, ICANN developed a consensual definition of abuse, according to which: "Abuse is an action that: a) causes actual and substantial harm, or is a material predicate of harm, and b) is illegal or illegitimate, or is otherwise contrary to the intention and design of a stated legitimate purpose, if such purpose is disclosed." (cited in Mahler, 2019, p. 251). More recently, in 2018, ICANN's Competition, Consumer Trust and Consumer Choice (CCT) Review team referred to "DNS Abuse" as "intentionally deceptive, conniving, or unsolicited activities that actively make use of the DNS and/or the procedures used to register domain names", whereas the term "DNS Security Abuse" refers to "more technical forms of malicious activity, such as malware, phishing, and botnets, as well as spam when used as a delivery method for these forms of abuse" (GAC, 2019, p. 2).

From a legal perspective, the abuse-notion as well as its suggested definitions are problematic, given the blurry lines between abuse and legitimate behaviour (Mahler, 2019, p. 251) *vis-à-vis* the much clearer distinction between lawful and unlawful behaviour or content. The European Commission, for example, defines illegal content as "any information which is not compliant with Union law or the law of a Member State concerned".[5] If abuse goes beyond that, however, it is unclear based on what standards or evaluations such a definition is based on and what this entails for procedural transparency, legal certainty and the rule of law.[6]

For the sake of clarity, I propose to differentiate in the context of domain names and the DNS between *abuse on the DNS* (i.e., content abuse such as content on a website accessible via a domain name), on the one hand, and *abuse of the DNS* (i.e., technical abuse such as turning a domain name into a bot) on the other hand. This distinction is first and foremost necessary given the "proximity" of abuse to the registry's functions. Whereas *technical* abuse has a more direct connection to the technical administrative role of registries and the DNS, *content* is much farther from a registry and the DNS given that the content is hosted elsewhere and merely being made more easily accessible by translating numerical IP addresses to human-readable alphanumerical domain names (see also Internet & Jurisdiction, 2019b, p. 6, pp. 20-21). Furthermore, the distinction also matters when looking at the efficiency of such enforcement tool: whereas *technical* abuse can in certain instances be brought to an end, domain name-related measures for *content* related reasons are a much more blunt and at the same time ineffective tool: the domain name as well as associated services such as email are made inaccessible on a global scale, whereas the content stays online where it is hosted and is just more difficult to access.

WHAT IS THE USE OF A DOMAIN NAME?

Related to the notion of "abuse" is the notion of "use". Before I take a closer look at the specific provisions in the ToS, it is noteworthy that quite a few ToS include a use-related provision in one way or another, while "abuse" is not a common notion in the analysed ToS. The question is, however, what the *use* of a domain name relates to. Here, we can differentiate between two layers: Firstly, as noted in the introduction, the use of a domain name could simply refer to the use of a domain *name* as such. In a narrow understanding this might not even include the technical use. Secondly, the use of domain name could also refer to the *use* of a domain name for a certain purpose, be it on the technical (*use of the DNS*) or on the content level (*use on the DNS*): for the layman this regularly has the purpose to make a certain website accessible via a domain name or enable email capabilities. This differentiation is crucial because the former relates only to the DNS, whereas the latter also relates to the underlying website content which is accessible, or activity via a domain name (Vissers et al., 2017; Schwemer, 2018).

The ToS of the UK registry administering <.uk>, Nominet, for example, stipulate "that you will not use the domain name for any unlawful purpose" (section 6.1.5). This compares to the ToS of German registry <.de>, DENIC, which calls for termination if "the registration of the domain for the Domain Holder manifestly infringes the rights of others or is otherwise illegal, regardless of the specific use made of it" (§ 7(2) d)). The German terms, thus, need to be understood in a way that relates to the domain name *as such* and not its use. At first glance this somewhat contradictory provision is introduced in the section on the *duties* of the registrants, where it is stipulated that a registrant gives an explicit assurance "that the registration and *intended use* of the domain does not infringe on anybody else's rights nor break any general law" (§ 3(1); emphasis added). In both ToS, regarding <.uk> and <.de>, there exists no further definition of "purpose" or "intended use".

The Norwegian registry, NORID, administering <.no>, does not directly refer to the *use* of a domain name in its terms, but requires a confirmation by the registrant declaring that "[the] use of the domain name (…) does not conflict with Norwegian law (…)" (declaration form appendix G 3.0, dated 22 May 2018). In these instances, however, it seems that the context – rather than keeping open a backdoor for a (non-judicial) takedown of a domain name for breach of terms – is meant to keep the registry free of liability.

Also the ToS of the <.eu> ccTLD registry, EURid, contain an ambiguous clause in the section on obligations of the registrant that could be interpreted in a way that the "use" can be understood broadly: the registrant has the obligation "not to use the Domain Name (i) in bad faith or (ii) for any unlawful purpose" (section 3 (3)). The terms further stipulate that the registry may revoke the registration inter alia if there is a "breach of the Rules by the Registrant" (section 8 (5) (iii)). In direct email follow-up with EURid, the registry however declared that it never takes action based on content associated with a domain name.[7] The ToS of the Hungarian ccTLD, <.hu>, similarly stipulate that the applicant is "to act with utmost care in selecting the domain so as the domain name (...) and the use of it shall not violate the rights of other persons or entities (...)" (section 2.2). It sets forth that a domain may be suspended if "the domain and/or the use of the domain name causes trouble in the operation of the Internet, or seriously threatens the security of the users" (section 5.2 b). In these instances, it appears from the wording that the provisions indeed enable the registry to intervene based on content or use of the domain name.

The <.be> registry's ToS also contain a "violation of law clause", where it specifies a condition that "the domain *name* is not used in violation of any applicable laws or regulations, such as a name that helps to discriminate on the basis of race, language, sex, religion or political view" (section 8 (a) (4); emphasis added). Looking at the list of examples, it appears that the use of a domain name is related to the name *as such*. At the same time, "such as" implies that the list is non-exhaustive. Thus, arguably, the use of the domain name in relation to content could be encompassed by the clause. This is supported by another broader clause in the <.be> terms that stipulates that the domain name is "not registered for any unlawful purpose" (section 8 (a) (3)).

Another peculiar provision can be found in the Croatian ordinance governing <.hr>, stipulating that "[t]he user of the domain shall *use* it only for the purpose for which it was registered and in a manner usual within the world Internet communities" (Article 24(3); emphasis added). In the ordinance, there exists, however, little guidance as to what this would entail.

In conclusion, in some instances it is only in the context of the specific terms, where an adequate interpretation can be found. Not only can it be difficult to understand whether the respective, often ambiguous, clauses only refer to the name *as such* or encompass also technical abuse or content abuse. The ambiguity of terms in the ToS is also furthered by their difficult readability (see also Bygrave, 2015, p. 5). In order to assess the readability of terms, the Flesch-Kincaid Grade Level score, based on sentence length and word length, is a common measure applied in research related to terms (Graber, D'Alessandro, & Johnson-West, 2002; Culnan & Carlin, 2006; Fiesler, Lampe, & Bruckman, 2016). The Grade Level Score for the analysed terms averages 13,8 (lowest: 10,8 (<.nl>); highest: 16,3 (<.ee>)) with a word count average at 6.200 words (lowest: 1.935 (<.ro>); highest: 22.839 (<.gr>), second highest 11.682 words (<.sk>)), making them difficult to very difficult texts to read. It seems problematic that terms are not clearer, though they are notably not as complex as many privacy and copyright policies, which average in the 14-15 range (and this article with a score in the 13 range).

WHAT DO THE TERMS SAY?

Several ccTLD registries, in their ToS, specify takedown mechanisms for use-related reasons. The terms regularly stipulate procedures in those instances and vary in scope. Based on the comparison of terms of the 30 examined ccTLD registries, they can roughly be grouped into three categories: (1) *broadly addressing use or content*, (2) containing *specific use- or content-related provisions*, and (3) *not addressing use of domain name or content* at all.

Firstly, several ToS contain *broad provisions* related to the illegality of content or use of the domain name, ranging from use for unlawful purposes to clear violations or manifestly illegal acts (Table 1).

Table 1: Broad provisions addressing use or content

Provision	ccTLD
Public order	<.nl>
Unlawful or illegal use	<nl.>; <.uk> ("any unlawful purpose"); <.be> ("not registered for an unlawful purpose"); <.ie>; ("used for any unlawful purpose"); <.eu> ("any unlawful purposes")
Used in bad faith	<.ie>; <.eu>
Clear violation of law	<.se>; <.dk> ("manifestly illegal acts")

Secondly, several terms of ccTLD registries refer to *specific cases* of unlawful or unwanted use of a domain name, ranging from decency and offensive content to the distribution of viruses and malware, phishing and denial of service and botnet attacks (Table 2).

Table 2: Specific provisions addressing use or content

Provision	ccTLD
National or international information security	<.sk>; <.cz> ("national or international computer security")
Serious threat to security of users	<.hu>
Obvious risk of economic crime	<.dk>
Compromising of IT equipment	<.dk>
Content of a highly offensive nature	<.dk>
Decency	<.nl>
Distribution of viruses and malware	<.uk>, <.ch> ("malicious code"); <.dk>; <.sk>; <.cz>
Phishing	<.uk>; <.sk>; <.cz>; <.dk>, <ch> ("obtain sensitive data by wrongful means")
Manage a network of devices infected without authorisation for the purpose of executing illegal activity (mainly botnet)	<.sk>; <.cz>
Facilitating distributed denial of service attacks	<.uk>

One third (11 out of 30) of the examined terms include a clause that somehow relates to use or content available under the domain name. Seven terms (7 out of 30) include at least one broad clause related to the illegal use of the domain name ("any unlawful purpose", "public order", "clear violation of law", usage in "bad faith", etc.), of which less than half (3 out of 7) also contain a specific use provision. The Swedish <.se>, the Irish <.ie>, the Belgian <.be> and the European <.eu> terms contain only a broad provision without a specific use provision, and only the Swiss <.ch> and the Hungarian <.hu> terms contain a specific use provision, but no general clause.

It is unclear whether the broad clauses (Table 1) are restricted to technical abuse or also envisioned to encompass content on the underlying website.[8] Roughly one fifth of the terms and conditions (seven out of 30), contain specific non-exhaustive catalogues of unlawful uses (e.g., phishing, malware distribution, botnets). These appear to primarily relate to technical abuse scenarios. Notably, however, the Dutch <.nl> ToS provide for a decency-related and the Danish <.dk> ToS for a "highly offensive nature" content-related provision; depending on the interpretation and the national legislative context, these provisions may not only regard unlawful but even unwanted content or use. Arguably, they leave the sphere of illegal behaviour open for a contractual basis for actions based on softer categories that go beyond illegal content or cybercrime. In recent policy debates, especially the violation of intellectual property rights, notably copyright and trademark infringements, as well as online shops selling counterfeit products have been topical. Despite this increasing pressure by stakeholders on actors, none of the analysed terms include a provision explicitly relating to these forms of use or content of the underlying website.

The two categories, broad and specific use-related, compare to a large number of registries (19 out of 30), which do not appear to include any use- or content-related provisions in their ToS (e.g., <.es>, <.mt>, <.lu>, <.lt>, <.lv>, <.ro>, <.si>, <.gr>, <.fr>, <it>). On the procedural side, some terms explicitly state that takedown only happens in case of a court order, arbitration or due to wrong information (e.g., <.at>, <de.>, <.pt>). Looking at the volume of registered domain names per registry, the picture looks different though: for 47,04 % of registrants (of the 61,67 million domain names), there exists some contractual basis pertaining to the use of a domain name (categories 1 and 3). This can be explained by the presence of larger and medium sized ccTLD spaces, notably <.uk>, <.nl>, and <.eu>.

It is outside the scope of this article to explore the reasons to include content- or use-related provisions in ToS. These might be influenced by legislation or jurisprudence (e.g., in relation to secondary liability), policymaking or independent commercial considerations by the respective registry or a result of co-regulation (Frydman, Hennebel, & Lewkowicz, 2012). In many instances, though, registries have a broad freedom to define the rules in their ToS. In Denmark, for example, the legislator has chosen a framework legislation, which gives the national registry a broad authority to define, when domain names should be suspended. In 2019, for example, the Danish registry conducted a hearing asking its stakeholders *inter alia* whether it should "be proactive and suspend domain names for websites that is known for phishing or malware spread" and "be able to suspend any domain name used in connection with the obvious risk of certain serious types of crime".[9] Some situations are also special, in that use-related provisions directly stem from administrative decrees or secondary legislation, as in the case of the <.fi> registry, which is a government agency, in the case of the Swiss registry, Switch, administering <.ch> and <.li>, the Greek registry <.gr>, and in the case of the Spanish registry, red.es, administering <.es>. In addition to the variety of setups and legal frameworks, the absence of a clear liability exemption framework within the E-Commerce Directive[10] (Truyens & van Eecke, 2016; Schwemer, 2018) might explain the differences in registries' approach to use of a domain name and content. An upcoming review of the E-Commerce Directive and the anticipated proposal of a Digital Services Act, according to leaked documents from DG Connect (European Commission, 2019), is envisioned to specifically address the liability exemption regime in relation to the DNS arguing that "clarification (...) is necessary".[11]

One central insight, however, is that the European landscape is heterogenous and divided into two major streams at this time: registries that address use or content in their terms to some extent, and registries that do not. There is little information available on a trend or historical evidence. Many ToS have been updated within the last two years, often due to the General Data

Protection Regulation[12] (GDPR) and its implications on WHOIS-databases (see e.g., Hoeren & Völkel, 2018). Yet, it seems plausible that content-related provisions have been more prominent in recent years, given the rise of general online content regulation discussions.

HOW ARE THE TERMS APPLIED?

As seen, some ToS potentially provide a contractual basis for the non-judicial domain name takedown for use- or content-related reasons by a registry. Another interesting question is whether and how domain registries make use of these provisions in practice. The analysis above says little regarding in which instances these provisions are or have been applied, but rather gives a picture of the contractual room of operations for ccTLD registries.

Some registries stipulate in their terms more or less directly that they do not assess the use of a domain name or content of websites made accessible via a domain name (see above). The German <.de> terms, for example, note that "[a]t no time is there any obligation whatsoever on DENIC to verify whether the registration of the domain on behalf of the Domain Holder or its use by the Domain Holder infringes the rights of others" (§ 2). The Austrian <.at> terms clarify that a revocation only takes place "in the case of a legally effective ruling by a court of law or a court of arbitration which is enforceable in Austria, and in the case of an instruction from a competent authority" (Section 3.8). In other instances, domain registries have set up trusted flaggers or trusted notifier regimes, where registries rely on notices by a public authority or private notifiers (Bridy, 2017; Schwemer, 2019).

Sometimes registries provide additional information on the handling of use or content on their website. But generally, information on practice related to the enforcement of use- or content-related terms in their ToS is – beyond sporadic press releases by registries – sparse and often not publicly available. Given that there is relatively little written and reported on such handlings, presumably the takedown of domain names directly based on an assessment of *content* – whether *ex officio* or on the motion of third parties – is rare. Or, at least, false positives might be rare, as infringers are unlikely to challenge the takedown of a domain name for use- or content-related reasons, which in turn could mean that there are few instances where the takedown of domain names for these reasons is challenged by the registrant.[13]

It is also difficult to assess the relation of domain registries to content without acknowledging the fluid boundary between content- and non-content-related measures. For example, when the legality of a domain name *as such* is determined, e.g., in connection with Uniform Domain-Name Dispute-Resolution Policy (UDRP) proceedings, the name *as such* is regularly the starting point. However, its *use* also constitutes one determining factor, even though the decision is not based on the content accessible via a domain name. Thus, the borders between content-related and purely domain name-related issues might be blurrier than they appear.

In the absence of concrete information from practice, I refer in this article to publicly available evidence related to the structural setup of content- or use-related mechanisms put in place by registries. In the following, I provide three examples that are noteworthy.

NOTICE-AND-TAKEDOWN MECHANISMS

The first example is the Dutch ccTLD registry administering <.nl>, SIDN, which established a notice-and-takedown procedure - akin to the procedures established by online platforms in connection to Article 14 of the E-Commerce Directive - for offending content that is clearly unlawful or criminal (CENTR, 2019b, p. 20; SIDN, 2019a). Anyone with a "legitimate interest" can, after having contacted the uploader, website manager, registrant, and registrar, request the registry to disable a <.nl> domain name. SIDN specifies in its takedown form, that they "take action only to prevent clearly unlawful or criminal activity. If, for example, expert legal opinion is needed to decide whether an activity is unlawful or criminal, we won't do anything." According to SIDN's yearly report (SIDN, 2019b, p. 9), the registry received 35 notice-and-takedown requests in 2018, of which seven led to the disabling of a domain name by SIDN. Given the low number of cases and the information on the setup of this mechanism it appears as a last-resort measure. Yet, it is a noteworthy mechanism which appears to be inspired by mechanisms put in place in relation to the liability exemption regime for hosting-providers from the E-Commerce Directive.

Somewhat related to these developments, is the establishment of trusted notifier regimes. A practice, that is increasingly seen and also encouraged by the European lawmaker,[14] is the offering of an expedited process for notices coming from "trusted flaggers" or "trusted notifiers". Some gTLD and some ccTLD domain registries have established such mechanisms (Bridy, 2017; Schwemer, 2019). Again, public information on the setup or workings, however, is sparse.

PROACTIVE SCREENING

The second example relates to the proactive screening of domain name *use* or *content*. Certain registries scan or proactively monitor the *usage of* and *content accessible under* a domain name for abuse. Technically, this is performed by for example crawling content, fuzzy hashes, HTML structural similarity analysis (see Gowda & Matmann, 2016) or analysis of registration data. In 2017, for instance, the <.eu> registry, EURid, introduced an abuse prevention tool using machine learning algorithms ("Abuse Prevention and Early Warning System") that flags suspicious domain name registrations and aims to prevent such maliciously used domain names from being active in the first place (EURid, 2016; EURid, 2017; EURid, 2019). The Belgian registry administering <.be>, DNS Belgium, also appears to have some kind of screening process outsourced to external security firms in place, which seems to primarily relate to technical abuse by third parties "for fraudulent practices such phishing, malware, etc." (DNS Belgium, 2019a). Also the Dutch registry administering <.nl>, SIDN, has put some research efforts into domain abuse and developed a domain early warning system for TLDs, which is "capable to detect several types of domain abuse, such as malware, phishing, and allegedly fraudulent web shops" (Moura, Müller, Wullink, & Hesselman, 2016). A concern in relation to proactive screening relates to the risk of false positives and the potential lack of competence to assess the legality of the allegedly infringing content.[15]

DATA VALIDATION

Accurate data has historically been necessary in order to get in touch with registrants with a view to solve technical issues; nowadays, however, there is a somewhat alternative use of data accuracy emerging in relation to abuse. Some have identified a plausible correlation between domain names that are used for unlawful purposes and the quality of the registration data (DK Hostmaster, 2019; Palage, 2019). Regularly, domain registries reserve the right to terminate a registration that is based on wrong or inaccurate information in their ToS (e.g., <.be>, <.se>, <.nl>, <.dk>, <is>, <.eu>, <.it>). Securing correct registrant information has been identified as one means to mitigate the problem.

Several registries have introduced internal or external data validation processes (e.g., <.dk>, <.uk>, <.eu>). The UK ccTLD-registry, Nominet, for example, uses a data validation process, where it matches name and address against a third-party data source (Nominet, 2019).

Similarly, the Belgian registry performs a daily manual screening of newly registered domain names, which is "carried out first and foremost to identify any obvious cases of *phishing* rapidly" (DNS Belgium, 2019b). In Denmark, a problem with online shops selling counterfeit products was manifested by an increasing number of court orders that the registry received to seize <.dk> domains. In 2017, the Danish registry, DK Hostmaster, introduced the mandatory use of a common login and verification solution used by government, banks and other private actors for identity verification purposes of Danish registrants and a risk-based assessment of foreign registrants at the time of registration. The verification requirement resulted in a decrease of online shops suspected of IP infringements from 6,73% to 0,12% (DK Hostmaster, 2019). Also, the <.eu> registry, EURid, cross-checks registration data with third parties, which by 2016 had resulted in the deletion of 31,819 domains at the registry's own initiative (EURid, 2016).

This offers an intriguing, somewhat creative, practical solution to the practical problem of unlawful use and content, which comes from a very different starting point: instead of a problematic move of registries towards effectively performing content policing, a reduction in "abuse" – whether technical or content-related – is merely a by-product of ensuring correct registration data. The Danish registry, for example, is, according to § 18(2) of the Danish domain name law *domæneloven* (*lov om internetdomæner, LOV nr 164 af 26/02/2014*) obliged to ensure correct, up-to-date and publicly available registration data in the WHOIS.[16] Whereas a specific obligation based on secondary legislation like the Danish example is rare, most analysed ccTLD registries address correct registration data in their ToS (see above).

Inaccuracy of registration data in this context is not evidence of malpractice but rather the reason for a domain name takedown in itself. In other words, the takedown of a domain name for technical reasons or content abuse is performed without the registry having to perform a legal evaluation of the use or the content on the underlying website. Thus, such a mechanism is – compared to trusted notifier regimes or takedown based on some kind of use or content analysis – also much less problematic from a fundamental rights perspective.

CONCLUSION

A report by the Internet & Jurisdiction policy network notes that a common challenge among all actors is "to define when is it appropriate to act at the DNS level in relation to the content or behavior of a domain address, and to identify the respective roles that courts and so-called 'notifiers' should play" (Internet & Jurisdiction, 2019a, p. 159). This analysis of 30 European ccTLD terms of services shows that there is a relatively wide spread of responses to use- and content-related domain name "abuse": some actors refrain from contractually reserving to takedown a domain name due to its *use* or *content*. Others reserve a right to take down a domain name in certain severe situations. Still others have established some kind of takedown-regime, akin to notice-and-takedown regimes of other intermediaries, or even introduced some form of proactive screening. A little more than a third of the analysed ccTLD terms contain content- or use-related provisions, accounting for 47,04% of the analysed ccTLD market. This compares to findings of Kuerbis, Mehta, & Mueller (2017), which found for registrars that 59% of terms comprise morality clauses accounting for 62% of the domain name market. Thus, the discretion for registrars to take down domain names is higher than for ccTLD registries. Yet a different market response by ccTLD registries to the issue of unlawful content appears to be the "creative use" of data validation. Without directly regulating use or content, this practice constitutes a practical solution for minimising the use of domain names for unlawful purposes.

Domain name takedowns based on privatised enforcement and self-regulation for content-related reasons are worrisome from a fundamental rights perspective (Kleinwächter, 2003; Seltzer, 2011; DeNardis, 2012; Schwemer, 2019) and risks and drawbacks associated with use- or content-related domain name takedowns have been identified elsewhere (see e.g., Schwemer, 2018; CENTR, 2019b, p. 14–15; Internet & Jurisdiction, 2019a, p. 159). It has for example been argued that "requests for domain name suspension should only be considered when one can reliably determine that a domain is used with a clear intent of significant abusive conduct; only a particularly high level of abuse and/or harm could justify resorting to such a measure" (Internet & Jurisdiction, 2019a, p. 159). In October 2019, a group of registrars and registries, notably including the registry administering the ccTLD <.uk>, released a "Framework for DNS Abuse",[17] arguing that "[d]espite the fact that registrars and registries have only one blunt and disproportionate tool to address Website Content Abuse, we believe there are certain forms of Website Content Abuse that are so egregious that the contracted party should act when provided with specific and credible notice". Notably, they argue that a registry or registrar should even without a court order address "content abuse" related to "child sexual abuse materials", the "illegal distribution of opioids online", "human trafficking" and "specific and credible incitements to violence". While domain registries have historically not been designed to engage in use- or content-related enforcement, recent developments seem to suggest that lines are getting blurrier between the infrastructure and the content layer of the internet.

A silent drift by domain registries into regulating and enforcing abusive content or activity on underlying websites – i.e., *use* and *content* regulation – is problematic. As seen in this article, many ToS are rather imprecise on the question what leeway they actually give for this kind of intervention by the registry. Furthermore, whereas information on the existence of such use- or content-related provisions is accessible via ToS, it says little about their practical application and importance. For the sake of transparency and legal certainty though, registries should be precise in their stance on the issue. European case law on domain registries and unlawful content too, is sparse.[18]

In this article, I have purposely focused on publicly available information only. In privatised enforcement systems, transparency is central to ensuring well-functioning and well-balanced regimes. Future research endeavours might benefit from further empirical work, for example by interviewing registries on their practices. It will also be relevant to revisit the ToS of registries in due time as the contractual basis for these measures might change. In direct follow-up with selected ccTLD registries, it appears that they are of minor practical relevance at this time. Given the topicality of content regulation, my expectation is that this practice will become more prevalent rather than disappear. In this trajectory, in any case, domain registries should be clear and transparent regarding their role in content- or use-related domain name takedowns.

ACKNOWLEDGEMENTS

This article is the result of a research project that has been funded by the Innovation Fund Denmark and the Danish Internet Forum (DIFO). I thank student assistant Berdien van der Donk for help with information collection. I thank Thomas Riis and Henriette Vignal-Schjøth for their comments on a draft of this paper, Kenneth Merrill and Farzaneh Badiei for their thorough and constructive peer-review, as well as Francesca Musiani and Frédéric Dubois for comments and suggestions. This research represents solely the view of the author. The author enjoyed full academic freedom but acknowledges that research results may be in the interest of the co-funding organisation.

APPENDIX

Analysed terms of services of ccTLDs. All registries have been checked for information last on 24 June 2019. Numbers marked with an asterisk (*) are retrieved from <http://research.domaintools.com/statistics/tld-counts/>, in instances where registries did not provide publicly available statistical information. The Flesch-Kincaid level has been calculated using a Microsoft Word script.

ccTLD	Country	Registry	Terms and conditions	Domains	Word count / words per sentence	Flesch-Kincaid Grade level
<.at>	Austria	nic.at	General Terms and Conditions, nic.at GmbH, AGB 2018; Version 3.2 of 16 May 2018	1.305.633	3.152 / 20,6	12,6
<.be>	Belgium	DNS Belgium	Terms and conditions for .be domain name registrations; Version 6.1 of 6 April 2018, Applicable as of 25 May 2018	1.501.401*	4.197 / 24,9	14
<.ch>	Switzerland; Liechtenstein	SWITCH	General Terms and Conditions (GTC) for the registration and administration of domain names under the domain ".ch" and ".li"; Entered into effect 1 January 2015 (Version 10)	289.991	5.111 / 21,9	13,2
<.cz>	Czech Republic	CZ.NIC	Rules of Domain Names Registration under the .cz ccTLD; Effective from 25 May 2018	1.326.646	9.912 / 15,5	11,9
<.de>	Germany	DENIC	DENIC Domain Terms and Conditions; (Retrieved 1 June 2019)	16.243.653	2.382 / 30,4	15,5
<.dk>	Denmark	DK Hostmaster	Terms and conditions for the right to use a .dk domain name; version 09 (Retrieved 1 June 2019)	1.320.622	3.482 / 25,5	13,2
<.ee>	Estonia	Estonian Internet Foundation	Domain regulation; Approved by the Estonian Internet Foundation Council on 7 March 2018 and taking effect on 25 May 2018	122.216	6.773 / 26,5	16,3

ccTLD	Country	Registry	Terms and conditions	Domains	Word count / words per sentence	Flesch-Kincaid Grade level
<.es>	Spain	Red.es (part of government)	*Ministerial Order ITC/1542/2005, dated 19 May, approving the National Plan for Internet Domain Names under the country code for Spain (".es") came into effect on 1 June 2005 and Instruction from the General Manager of the Public Business Entity Red.es, which outlines the procedures applicable to assignment and other operations associated with registering ".es" domain names; dated 8 November 2006*	1.918.039	N/A	N/A
<.eu>	European Union	EURid	Domain Name Registration Terms and Conditions, v.10.1 [accessed 1 June 2019]	3.661.899	3.929 / 21,5	13,1
<.fi>	Finland	Traficom	*Domain Name Regulation*; issued in Helsinki 15 June 2016	444.958*	N/A	N/A
<.fr>	France	Afnic	Naming Policy for the French Network Information Centre; Rules for registering Internet domain names using country codes for metropolitan France and the Overseas Departments and Territories, Version 25 May 2018	3.396.646	7.112 / 21,9	14,4
<.gr>	Greece	FORTH-ICS	*Regulation on Management and Assignment of [.gr] or [.ελ] Domain Names, Decision 843/2 of 1-3-2018 by The Hellenic Telecommunications and Post Commission (EETT)*	396.102*	22.839 / 25,6	14,2
<.hr>	Croatia	CARNet	*Ordinance on the Organisation and Management of the National Top-level Domain*	98.094*	8.357 / 27,8	16,1
<.hu>	Hungary	Council of Hungarian Internet Providers	Domain registration rules and procedures; Effective as of 25 May 2018	748.423	9.585 / 28,1	16,9

ccTLD	Country	Registry	Terms and conditions	Domains	Word count / words per sentence	Flesch-Kincaid Grade level
<.ie>	Ireland	IEDR	Registrant Terms and Conditions – Effective from 1 July 2019	262.140	7.429 / 22,8	13,2
<.is>	Iceland	ISNIC	Terms and Conditions; 1 November 2011 [accessed 1 June 2019]	68.003	2.986 / 16,4	11,4
<.it>	Italy	Registro.it	Assignment and management of domain names in the ccTLD .it; Regulation; Version 7.1; 3 November 2014	3.202.835	9.600 / 23,6	
<.lt>	Lithuania	DOMREG	Procedural Regulation for the .lt Top-level Domain; Edition 2.0; Version 2.1; 25 May 2018	195.036	6.433 / 14,1	12,1
<.lu>	Luxembourg	Fondation RESTENA	Terms and Conditions of Classic Registration and Management of .lu Domain Names; Version 6.0, May 2018	99812	7.536 / 23,5	14,0
<.lv>	Latvia	NIC.LV	Policy for acquisition of the right to use domain names under the top level domain .lv; amended as of 17 May 2019 (enters into force on 22 May 2019)	110.350*	4.064 / 13,9	11,4
<.mt>	Malta	NIC-MT	Terms and Conditions; effective from 1 December 2017	18.258*	2.395 / 28,2	15,3
<.nl>	Netherlands	SIDN	General Terms and Conditions for .nl Registrants; 1 May 2019	5.872.244	5.559 / 16,1	10,8
<.no>	Norway	Norid	Domain name policy for .no; Last change: 8 January 2019	710.892*	4.710 / 18,5	12,3
<.pl>	Poland	NASK	.pl Domain Name Regulations as of 18 December 2006 (In force as of 1 December 2015)	2.605.818	2.860 / 29,6	15,7
<.pt>	Portugal	DNS.PT	21 May 2018	1.150.283	7.565 / 26,5	15,7
<.ro>	Romania	Internet Service Romania	Domain Name Registration Agreement; Version Number: 4.0 [09/2000]	496.030*	1.935 / 25,8	14,7

ccTLD	Country	Registry	Terms and conditions	Domains	Word count / words per sentence	Flesch-Kincaid Grade level
<.se>	Sweden	Internetstiftelsen	Terms and Conditions of Registration applicable for the top-level domain .se from 6 February 2019	1.510.883	3.738 / 21,2	14,5
<.si>	Slovenia	Arnes	General Terms and Conditions for Registration of Domain Names under the .SI Top-Level Domain; Publication 1 July 2016, validity from 1 August 2016	132.641	5.844 / 14,2	11,4
<.sk>	Slovakia	SK-NIC	Terms and Conditions of Domain Name Service in .sk Top Level Domain; 1 October 2018	394.776	11.682 / 24,6	15,0
<.uk>	United Kingdom	Nominet	Terms and Conditions of Domain Name Registration (n.d.)	1.2168.405	2.699 / 25,9	13,9

REFERENCES

Aguerre, C. (2010). *ccTLDs and the local dimension of Internet Governance* [Working Paper No. 8]. Buenos Aires: Centro de Tecnología y Sociedad UdeSA. Retrieved from http://hdl.handle.net/10908/15557

Belli, L., & Venturini, J. (2016). Private ordering and the rise of terms of service as cyber-regulation. *Internet Policy Review*, *5*(4). https://doi.org/10.14763/2016.4.441

Bettinger, T., & Waddell, A. (Eds). (2015). *Domain Name Law and Practice*. Oxford: Oxford University Press.

Bridy, A. (2017). Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation. *Washington and Lee Law Review*, *74*(3), 1345–1388. Retrieved from https://scholarlycommons.law.wlu.edu/wlulr/vol74/iss3/3/

Bygrave, L. (2015). *Internet Governance by Contract*. Oxford: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199687343.001.0001

Bygrave, L., Schiavetta, S., Thunem, H., Lange, A. B., & Phillips, E. (2009). The naming game: governance of the Domain Name System. In L. Bygrave & J. Bing (Eds.), *Internet Governance: Infrastructure and Institutions* (pp. 147–212). Oxford: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199561131.003.0006

Christou, G., & Simpson, S. (2007, September). *New Modes of regulatory governance for the internet? Country code top level domains in Europe*. European Consortium for Political Research General Conference, Pisa. Retrieved from http://www.regulation.upf.edu/ecpr-07-papers/ssimpson.pdf

Christou, G., & Simpson, S. (2009). New Governance, the Internet, and Country Code Top-Level Domains in Europe. *Governance*, *22*(4), 599–624. https://doi.org/10.1111/j.1468-0491.2009.01455.x

Council of European National Top-Level Domain Registries (CENTR). (2019a). *CENTRstats, Global TLD Report, Q1 2019 – Edition 27*. Retrieved from https://stats.centr.org/stats/global

Council of European National Top-Level Domain Registries (CENTR). (2019b). *Domain name registries and online content*. Brussels. Retrieved from https://centr.org/library/library/centr-document/domain-name-registries-and-online-content.html

Culnan, M. J., & Carlin, T. J. (2006). Online Privacy Practices in Higher Education: Making the Grade? *Communications of the ACM*, *52*(3) 126–130. https://doi.org/10.1145/1467247.1467277

DeNardis, L. (2012). Hidden levers of Internet control: An infrastructure-based theory of Internet governance. *Information, Communication & Society*, *15*(5), 720–738. https://doi.org/10.1080/1369118X.2012.659199

DK Hostmaster. (2018). *Crime prevention on the internet*. Retrieved from https://www.dk-hostmaster.dk/sites/default/files/2019-07/Internetcrime_onepager_050319_EN.pdf

DNS Belgium. (2019a). Misuse of your domain name. Retrieved from https://www.dnsbelgium.be/en/internet-security/misuse-your-domain-name

DNS Belgium. (2019b). Complaints on a domain name?. Retrieved from https://www.dnsbelgium.be/en/register-your-domain-name/complaints-domain-name

European Commission. (2019). *Digital Services Act note DG Connect June 2019*. Retrieved from https://cdn.netzpolitik.org/wp-upload/2019/07/Digital-Services-Act-note-DG-Connect-June-2019.pdf

EUIPO. (2018). *Comparative case study on alternative resolution systems for domain name disputes*. Alicante: European Intellectual Property Office. https://doi.org/10.2814/294649

EURid. (2016). *Abuse monitoring policies and procedures @ EURid*. Brussels, 28 Jan 2016. Retrieved from https://gac.icann.org/briefing-materials/public/eurid-2016-01-28.pdf

EURid (2017, October 2). EURid set to launch first of its kind domain name abuse prevention tool. Retrieved from https://eurid.eu/en/news/eurid-set-to-launch-first-of-its-kind-domain-name-abuse-prevention-tool/

EURid (2019). .eu means trust. Retrieved from https://trust.eurid.eu/de/

Fiesler, C., Lampe, C., & Bruckman, A. S. (2016). Reality and Perception of Copyright Terms of Service for Online Content Creation. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, 1450–1461. https://doi.org/10.1145/2818048.2819931

Frosio, G. (2017). *Why keep a dog and bark yourself? From Intermediary Liability to Responsibility* [Research Paper No. 2017-11]. Strasbourg: Centre for International Intellectual Property Studies. Retrieved from https://papers.ssrn.com/abstract_id=2976023

Frydman, B., Hennebel, L., & Lewkowicz, G. (2012). Co-regulation and the rule of law. In E. Brousseau, M. Marzouki & C. Méadel (Eds.), *Governance, Regulations and Powers on the Internet* (pp. 133-150). Cambridge: Cambridge University Press.

Governmental Advisory Committee (GAC) (2019, September 18). *GAC Statement on DNS Abuse*. Los Angeles: ICANN. Retrieved from https://gac.icann.org/file-asset/public/gac-statement-dns-abuse-final-18sep19.pdf

Geist, M. (2004). Governments and country-code top level domains: a global survey. Retrieved from https://www.itu.int/osg/spu/forum/intgov04/contributions/governmentsandcctldsfeb04.pdf

Graber, M. A., D'Allesandro, D. M, & Johnson-West, J. (2002). Reading Level of Privacy Policies on Internet Health Web Sites. *The Journal of Family Practice*, *51*(7), 642–645.

Gowda, T. & Matmann, C. A. (2016). Clustering Web Pages Based on Structure and Style Similarity (Application Paper). *2016 IEEE 17th International Conference on Information Reuse and Integration (IRI)*, 175–180. https://doi.org/10.1109/IRI.2016.30

Hao, S., Thomas, M., Paxson, V., Feamster, N., Kreibich, C., Grier, C., & Hollenbeck, S. (2013). Understanding the domain registration behavior of spammers. *Proceedings of the 2013 conference on Internet measurement conference*, 63–76. https://doi.org/10.1145/2504730.2504753

Hoeren, T., & Völkel, J. (2018). Information Retrieval About Domain Owners According to the

GDPR. *Datenschutz und Datensicherheit 2018*. https://doi.org/10.2139/ssrn.3135280

Internet & Jurisdiction Policy Network (2019a). *Global Status Report 2019*.

Internet & Jurisdiction Policy Network (2019b, April). *Domains & Jurisdiction Program; Operational Approaches, Norms, Criteria, Mechanisms*.

Kidmose, E., Lansing, E., Brandbyge S., & Pedersen, J. (2018). Heuristic methods for efficient identification of abusive domain names; *International Journal On Cyber Situational Awareness (IJCSA)*, *3*(1), 121–142. https://doi.org/10.22619/IJCSA.2018.100123

Kleinwächter, W. (2002). From self-governance to public-private partnership: The changing role of governments in the management of the internet's core resources. *Loy. LAL Rev.*, *36*, 1103.

Korczyński, M., Tajalizadehkhoob, S., Noroozian, A., Wullink, M., Hesselman, C., & Eeten, M. Van. (2017). Reputation Metrics Design to Improve Intermediary Incentives for Security of TLDs. *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, 579–594. https://doi.org/10.1109/EuroSP.2017.15

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

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

Malcolm, J., Rossi, G., & Stoltz, M. (2017). *Which Internet registries offer the best protection for domain owners?* [Report]. San Francisco: Electronic Frontier Foundation. Retrieved from https://www.eff.org/files/2017/08/02/domain_registry_whitepaper.pdf

Moore, T., Clayton, R., & Anderson, R. (2009). The Economics of Online Crime. *Journal of Economic Perspectives*, *23*(3), 3-20. https://doi.org/10.1257/jep.23.3.3

Moura, G. C. M., Müller, M., Wullink, M., & Hesselman, C. (2016). nDEWS: a New Domains Early Warning System for TLDs. *NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, 1061–1066. https://doi.org/10.1109/NOMS.2016.7502961

Mueller, M. (2010). *Networks and States: The Global Politics of Internet Governance*, Cambridge: The MIT Press.

Mueller, M., & Badiei, F. (2017). Governing Internet Territory: ICANN, Sovereignty Claims, Property Rights and Country Code Top-Level Domains. *Columbia Science & Technology Law Review*, *18*, 435–491. Retrieved from http://www.stlr.org/download/volumes/volume18/muellerBadiei.pdf

Mueller, M., & Chango, M. (2008, December 2). *Disrupting Global Governance: The Internet Whois Service, ICANN, and Privacy*. Third Annual GigaNet Symposium, Hyderabad. Retrieved from https://doi.org/10.2139/ssrn.2798940

Nominet (2019). How does Nominet validate data? Retrieved from https://registrars.nominet.uk/uk-namespace/data-quality-policy/how-does-nominet-validate-data/

Obar, J. A., & Oeldorf-Hirsch, A. (2018). The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128–147. https://doi.org/10.1080/1369118X.2018.1486870

Palage, M. (2019). *The Role of ccTLD Managers in the Evolving Digital Identity Ecosystem*. Brussels: Council of European National Top-Level Domain Registries.

Park, Y. J. (2008). *The political economy of country code top level domains* [Doctoral Thesis, Syracuse University]. Retrieved from https://surface.syr.edu/it_etd/9/

Riis, T., & Schwemer, S.F. (2019). Leaving the European Safe Harbor, Sailing Towards Algorithmic Content Regulation. *Journal of Internet Law*, *22*(7), 1–21.

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

Schwemer, S.F. (2018). On domain registries and unlawful website content: Shifts in intermediaries' role in light of unlawful content or just another brick in the wall? *International Journal of Law and Information Technology*, *26*(4), 273-293. https://doi.org/10.1093/ijlit/eay012

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

Seltzer, W. (2011). Exposing the flaws of censorship by domain name. *IEEE Security and Privacy*, *9*(1), 83–87. https://doi.org/10.1109/MSP.2011.8

SIDN (2019a). Complaining about the content of a website. Retrieved from https://www.sidn.nl/a/nl-domain-name/complaining-about-the-content-of-a-website?language_id=2

SIDN (2019b). *2018 Annual Report*. Retrieved from https://jaarverslag.sidn.nl/jaarverslag/pdf/SIDN_Annual_report_2018.pdf

Truyens, M., & van Eecke, P. (2016). Liability of Domain Name Registries: Don't Shoot the Messenger. *Computer Law & Security Review*, *32*(2), 327–344. https://doi.org/10.1016/j.clsr.2015.12.018

Vissers, T., Spooren, J., Atgen, P., Jumpertz, D., Janssen, P. ..., Desmet, L. (2017). Exploring the ecosystem of malicious domain registrations in the .eu TLD. In Dacier M., Bailey M., Polychronakis M., Antonakakis M. (Eds.), *Research in Attacks, Intrusions, and Defenses* (pp. 472–493). Springer. https://doi.org/10.1007/978-3-319-66332-6_21

FOOTNOTES

[1] On the problematic terminology see below.

[2] ccTLD registries of the European Economic Area (EEA), i.e., 28 EU member states and Iceland, Norway, Liechtenstein, plus Switzerland (which is EFTA member but not part of the EEA). All ToS have been analysed in their English translation provided by the registry; many ToS contain a clause whereafter the original language version prevails. All domain registries' ToS have been checked with a cut-off date of 15 June 2019. See Appendix for a full overview on

terms of services of ccTLDs.

3. See e.g., Article 4 nr. 15 and nr. 16 of 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, pp. 1–30.

4. See also Internet & Jurisdiction, 2019b, pp. 20–21, differentiating technical abuse, namely spam, malware, phishing, pharming, botnets and fast-flux hosting, and website content abuse, namely child abuse material, controlled substances and regulated goods, violent extremist content, hate speech, and intellectual property.

5. Commission Recommendation of 1 March 2018 on measures to effectively tackle illegal content online, C(2018)1177, European Commission, March 2018.

6. This resembles the blurry lines in a parallel discussion regarding platforms and proactive mechanisms, where for instance Frosio has commented on a shift from "liability to responsibility" (Frosio, 2017; see also Riis & Schwemer, 2019).

7. Email exchange with EURid legal department of 5.12.2018, on file with author.

8. See also discussion above.

9. Danish Internet Forum (2019). "Written hearing regarding the role of DIFO in the fight against online crime", Written hearing regarding the role of DIFO in the fight against online crime. Available at: https://www.dk-hostmaster.dk/en/news/written-hearing-regarding-role-difo-fight-against-online-crime

10. 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 [2000] OJ L 178, pp. 1–16.

11. See also Schwemer, S. (2019). "Domain Name System to Be Featured Prominently in Upcoming Review of EU Safe Harbor Rules". *CircleID,* 23 September 2019. Available at: http://www.circleid.com/posts/20190923_dns_to_be_featured_prominently_in_review_of_eu_safe_harbor_rules/

12. EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119, pp. 1–88.

13. On jurisprudence in Europe related to the liability of domain registries for content see my earlier work in Schwemer, 2018.

14. More specifically in the context of online platforms; see Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, 6 March 2018, [2018] L 63/50.

15. In relation to online platforms, for example, see the overview on empirical evidence on over-removal prepared by Daphne Keller, Empirical Evidence of "Over-Removal" by Internet Companies under Intermediary Liability Laws, *The Center for Internet and Society, Stanford Law School* (12 October 2015, last updated 14 September 2018), http://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-compan

ies-under-intermediary-liability-laws

[16] This is why the <.dk> WHOIS database remains publicly available, whereas many other registries have restricted access, see on the issue see Mueller and Chango, 2008; Hoeren and Völkel, 2018.

[17] *Framework to Address Abuse*, October 2019 (signed by Public Interest Registry, Donuts, Amazon Registry Services, Afilias, Amazon Registrar, Nominet UK, GoDaddy, Tucows, Blacknight Solutions, Name.com, Neustar), available at http://www.circleid.com/pdf/Framework_to_Address_Abuse_20191017.pdf

[18] I have explored this in earlier related research, see Schwemer 2018.