Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Liability of domain name registries: Don't shoot the messenger

M. Truyens [a,*], P. Van Eecke [a,b,c]

[a] Faculty of Law, University of Antwerp, Antwerp, Belgium
[b] King's College, London
[c] Institute of Computer and Communications Law, Queen Mary University of London, UK

Keywords:
DNS
Domain names
Intermediaries
Blocking
Hosting
Monitoring

ABSTRACT

The domain name system (DNS) is fundamental to the Internet, because it translates domain names to and from computer (IP) addresses. This system is, however, increasingly used as a tool to combat unwanted online content. In this process, the system's most central operators ("registries") are targeted by right holders, authorities and other claimants, even though the registries fulfil a mere technical role as an online intermediary, and are quite distanced from the actual content.

This contribution presents arguments why registries and other DNS-operators would be protected against several types of domain blocks, monitoring duties and liability claims. These arguments are not only supported by a forward-looking interpretation of the special protection regime for mere conduit, caching and hosting providers of the EU eCommerce Directive 2000/31/EC, but also by Enforcement Directive 2004/48/EC and general EU law, as interpreted by the Court of Justice of the European Union.

1. Introduction

Online intermediaries provide essential facilities, such as granting access to the Internet, transferring data, providing space to store data, and offering facilities to publish web sites. Throughout the evolution of the Internet, they have been in a special position, because they have much more visibility than their users, who can stay anonymous and can be very difficult to track down. Since their role is somewhat similar to the role of a newspaper publisher or book publisher, it was not surprising that courts – unfamiliar with the intricacies of the new online context – were inclined to impose the traditional rules of publisher liability on online intermediaries. As a result, courts started to consider intermediaries liable for actions committed by their users,[1] even though it was economically unfeasible or even technically impossible for them to monitor the information of all their users.

To rectify this situation and stimulate the uptake of online services, in Europe the eCommerce Directive[2] was enacted,

* *Corresponding author.* Faculteit Rechten, Universiteit Antwerpen, Venusstraat 23, 2000 Antwerpen, Belgium.
E-mail address: maarten.truyens@ua.ac.be (M. Truyens).

[1] For example, the general manager of CompuServe Germany was prosecuted for facilitating access to violent and child pornographic content stored in newsgroups accessible by CompuServe's customers (*Local Court [Amtsgericht] Munich*, File No.: 8340 Ds 465 Js 173158/95). In the United Kingdom, access provider Demon was held liable for not removing an offensive posting in one of the thousands of newsgroups (*Godfrey v. Demon Internet* [1999] 4 All ER 342). In the Netherlands, an operator of an electronic discussion forum was found liable for direct copyright infringement because he allowed subscribers to upload and download potentially pirated software (District Court of Rotterdam 24 August 1995, Informatierecht/AMI, 1996/5, page 101).

[2] Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Official Journal L 178, 17/07/2000).

http://dx.doi.org/10.1016/j.clsr.2015.12.018

which, among other elements, created a "safe harbor" so that certain categories of intermediaries would be protected against liability claims caused by their users, and could not be obliged to monitor the behaviour of their users.

This protection has worked fairly well for those intermediaries whose activities clearly match the wording of the Directive, such as Internet access providers and online storage space providers. Particularly after further clarification by the Court of Justice of the European Union (CJEU), many traditional online intermediaries can now assume to be reasonably protected against third liability claims.

However, unwanted content has continued to thrive online, and its removal has been intensified through case law[3] and various regulatory initiatives, both at the EU-level[4] and the national level.[5] Law enforcement agencies, authorities, right holders and prejudiced parties (hereafter jointly referred to as "claimants") have therefore started looking for additional courses of action. For example, individual users have been randomly but directly targeted by right holders with expensive lawsuits to achieve a dissuasive effect.[6] Warning schemes have been created, where Internet access providers forward gradually increasing notices of default to individual users.[7] Right holders have also started to send massive amounts of takedown notices to intermediaries.[8] On a voluntary basis, some online platforms have entered into agreements to install content filters.[9] Another course of action is to target other types of intermediaries who are positioned elsewhere in the online value chain,[10] such as backbone operators and payment providers[11] to cut off the funding of commercial-scale pirating.

Lately, operators who manage the Internet's domain name system (DNS[12]) have also become a target for claimants. As explained in further detail below, the DNS-system provides fundamental Internet functionality, similar to publishing the central phone book that allows subscribers to look up phone numbers. It has unfortunately evolved over the years from a merely technical infrastructure service to the *de facto* point of contact to take legal action by requesting information about persons behind Internet sites or services.

By requesting DNS-operators to remove, takedown or redirect domain names – hereinafter collectively called a "blocking" of a domain name – unwanted content can be easily hidden from the public. While the number of such requests is not yet substantial, it is clearly rising. As recently noted in relation to a German court order against a DNS-operator who was held liable for the copyright infringements

[3] For example, the "right to be forgotten", as applied by the CJEU in the *Google Spain* case (C-131/12, 13 May 2014). As a result, Google received 172,752 removal requests in less than six months (see goo.gl/d4zREa).

[4] See, for example, the Cybercrime Convention of 23 November 2001 (criminalising aiding or abetting of cybercrime); Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography; Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems; Council of the European Union, Framework Decision on combating racism and xenophobia, 28 November 2008; Council of the European Union, Revised Action Plan on Terrorism, 10043/06, Brussels, 31 May, 2006. For a more general overview on blocking initiatives, see Y. Akdeniz, "To block or not to block: European approaches to content regulation, and implications for freedom of expression", *Computer Law & Security Review* 2010, 26; W. Stol, H. Kaspersen, J. Kerstens, Leukfeldt, ER and A. Lodder, "Governmental filtering of websites: the Dutch case", *Computer Law & Security Review* 2009, 25.

[5] For example, in Germany, in 2002, North Rhine Westphalia issued a blocking-order against ISPs regarding racist and neo-Nazi content. In 2009, after strong political pressure, Germany's biggest ISPs signed an agreement with the government to block access to blacklisted pornography websites. In 2009, a bill with similar goals was passed. In the UK, in 2013, an agreement was reached between the government and the four largest ISPs to force subscribers to choose whether to activate "family-friendly network level filtering service" (blocking pornography, drugs, file sharing, violence, etc.). Separately, the "Internet Watch Foundation" aims to minimise the availability of images of child sexual abuse on the Internet by producing a list of URLs (made available to UK ISPs) that contain images of child abuse. In Denmark, a law was adopted in 2011 (but repealed in 2013) blocking access to websites selling illegal medicine. Filters are also installed in Norway since 2004, Sweden since 2005, Denmark since 2005 and the Netherlands since 2007. In Belgium, a blacklist of gambling sites has been effective since 2012 (see official list available on www.gamingcommission.be).

[6] For example, in the United States, the recording industry association (RIAA) initiated an anti-downloading litigation campaign. While most claims have been settled out of court, a few reached a verdict. The most high-profile case concerned *Sony BMG Music Entertainment* v. *Tenenbaum*, in which a jury awarded damages of $675.000 USD (later on reduced to $67,500) for a student's sharing of thirty music files online.

[7] See the "graduated response" (HADOPI legislation) adopted in France in 2009, which was revoked in 2013 because the measures were considered disproportionate. A similar system was proposed in 2009 in the United Kingdom, and has been effectively in force in the United States since 2013.

[8] For example, in November 2014, Google received takedown requests for over 36 million URLs relating to more than 50,000 different domains (see www.google.com/transparencyreport/removals/copyright/).

[9] YouTube installed the "Content ID" system (support.google.com/youtube/answer/2797370) which allows right holders to take down copyrighted files, or instead share revenue obtained from advertisements. Another example is eBay's "Verified Rights Owner" (VeRO) program for right holders to facilitate easier reporting of infringements (pages.ebay.com/help/policies/programs-vero-ov.html).

[10] L. Feiler, "Website block injunctions under EU and US copyright law – slow death of the global Internet or emergence of the rule of national copyright law?" TTLF Working Paper Nr. 13, available at goo.gl/u1QOm7.

[11] The so-called "follow the money" approach of the European Commission (cf. the Press Release on better protection and enforcement of intellectual property rights, 1 July 2014, available on europa.eu/rapid/press-release_IP-14-760_en.htm). In the same vein, for the United States, see the 2006–2007 US case *Perfect 10, Inc. v. Visa Int'l Serv. Ass'n* (494 F.3d 788 – 9th Cir. July 3, 2007), where the copyright holder claimed contributory copyright infringement and vicarious copyright infringement committed by credit card operators Visa and MasterCard.

[12] For the sake of brevity, and in order to stay aligned with common technical terminology, we will refer to the "domain name system" as the "DNS-system", despite the double use of the word "system".