Kluwer Copyright Blog

Duties of DNS resolvers and CDN providers – the CoA Cologne (Germany) finds Cloudflare accountable

Jan Bernd Nordemann (NORDEMANN) · Monday, July 12th, 2021


Image by Gerd Altmann from Pixabay

According to a recent Oberlandesgericht (Court of Appeal – CoA) Cologne ruling, providers of DNS resolvers may be held accountable to DNS block domain names used by websites which run an illegal business model dedicated to copyright infringements. Additionally, providers of content delivery networks (CDNs) have a duty to stop their services for such rogue websites. In the case, US based Cloudflare provided both DNS resolver and CDN services to the rogue website ddl.music.to. The judgment of 9 October 2020 (6 U 32/20) is available (in German) here.

DNS resolver providers

Some rogue websites have based their business model around copyright infringement. Such rogue websites are also called structurally infringing websites. They frequently cannot be prosecuted because they hide behind anonymity. It is more efficient – if not the only option – to require intermediaries providing services for the infringement to prevent further infringements.

DNS (domain name system) blocks are a tool commonly used where legal action against the operators and hosts would not be effective. A DNS block means that the provider of DNS resolvers will not comply with the request to resolve a domain name

typed into the browser into the IP address connected to this domain name. As a result, a user cannot access the requested website. Usually, internet users will use the DNS servers of their access provider. But internet users can also choose to use DNS resolvers from third parties like Cloudflare or Google.

It has been widely recognized that access providers operating DNS servers can be held accountable under the national implementations of Art. 8(3) InfoSoc Directive, following the leading CJEU judgment *UPC Telekabel*.[1]

But so far other *operators of DNS resolvers* have not been sued before courts to implement DNS blocks. For Cloudflare's DNS resolvers, the CoA Cologne held on 9 October 2020 that they are accountable as if they were an access provider operating a DNS server. The CoA Cologne based its ruling on the German implementation of Art. 8 (3) InfoSoc Directive, i.e. the German Stoererhaftung.

As the same rules applied as for access providers operating DNS servers, the court assessed parallel legal requirements.

- DNS resolver operators would provide services used for copyright infringement if they resolve domain names of structurally copyright infringing websites.
- There is a proportionality test weighing the constitutional rights to intellectual property and freedom to information. The CJEU held that the measures adopted by the internet service provider must be strictly targeted (CJEU para. 56 – *UPC Telekabel*). In particular, DNS blocks implemented in the DNS resolvers must not lead to overblocking of legal content available on such structurally copyright infringing websites. In the present case, the Cologne court found "exclusively illegal offers" on the website, so no overblocking was at stake.
- Finally, a German peculiarity applied, the so-called subsidiarity principle. This means that DNS blocks must be "last resort" after all proportionate measures against the operators and technical providers of the structurally copyright infringing website have been exhausted. This is the standing case law of the German Federal Supreme Court (BGH; see BGH of 26 November 2015, I ZR 174/14 – *Stoererhaftung des Accessproviders*. But it seems questionable whether this is in line with Art. 8 (3) InfoSoc Directive; some EU Member States have explicitly not used the subsidiarity principle (see here).

The case also confirmed that DNS blocks may be requested from DNS resolver operators residing abroad – even outside the EU. Such foreign DNS resolver operators will face duties of care as if they were domestic providers, because national law applies to the copyright infringements pursuant to Article 8 (1) Rome II Regulation. This is the case if the copyright infringement targets (at least also) the country of protection (in line with *Football Dataco/Sportradar*). In the present case, Germany was also the target of the rogue website.

The court order to DNS block was limited to the territory of Germany. Nevertheless, the DNS resolver operator argued that the order was inadmissible, as it could only be implemented worldwide. The court was not impressed by this argument. Even if an order to DNS block for internationally operated DNS resolvers restricted to Germany had overspill effects beyond Germany, this would not make the order inadmissible.

The website had no legal offer under German copyright law anyhow and it was not put before the court that the content was legal to a relevant extent in other copyright jurisdictions outside Germany.

Content Delivery Network (CDN) Providers

A content delivery network (CDN) offers various services to its customers. A CDN may be used as an anonymization service for operators of websites. CDN providers will provide their own IP address to the customer's website. The true IP address is no longer identifiable for third parties such as rightholders. All traffic is routed through the infrastructure of the CDN providers. The websites served are largely stored on the CDN's own servers. CDN providers will have direct or indirect contractual links to the website operator. In the Cologne case, the CDN services were used to anonymize the structurally copyright infringing websites and to hide the true IP address.

The Cologne court held that – after being put on notice – the CDN provider would be accountable pursuant to Stoererhaftung. CDN providers would not be access providers (within the meaning of Art. 12 E-Commerce Directive) nor cache providers (within the meaning of Art. 13 E-Commerce Directive). Rather, the CoA developed the duties of care developed in German case law for hosting providers. According to this case law, after having been notified of a clear copyright infringement, hosting providers have a duty of care to ensure takedown and staydown of the infringing content and also have to prevent infringements of the same kind which are just as clear (BGH of 13 September 2018, I ZR 140/15 para. 49 – *YouTube*). The CoA Cologne argued that such duties would be justified because CDN providers had contractual links to the infringers and could use the corresponding influence to stop infringements at the source.

No subsidiarity rule could be invoked by the CDN provider, as it was not in a role comparable to access providers or DNS resolver providers, as shown above.

The CoA limited its ruling to injunction claims under Stoererhaftung (Art. 8 (3) InfoSoc Directive). For procedural reasons, unfortunately the CoA did not have to answer the question raised by the rightholder: Would a CDN provider be liable as an infringer (including for damages) according to the CJEU case law in *Brein/Ziggo – "ThePiratebay"* and *Youtube/Uploaded*?

Outlook

Cloudflare and its anonymization services attract structurally copyright infringing websites. Also, Italian courts have ruled against Cloudflare in the past. The CoA Cologne judgment is one of the few in the EU which further shapes the duties of care under copyright law pursuant to Art. 8 (3) InfoSoc Directive for CDN providers. To apply comparable duties of care to CDN providers as to hosting providers seems correct. Like hosting providers, CDN providers have contractual links to copyright infringers who use CDN providers as their direct technical providers.

Regarding DNS resolver providers, the judgment confirms duties of care to DNS block, comparable to those for access providers. Indeed, it seems quite obvious that a DNS resolver operator should face the same duties as access providers operating DNS servers. This is true even if they operate internationally beyond national borders. The practical importance of such duties of DNS resolver operators to implement DNS blocks upon request by an infringed rightholder must not be underestimated. Important internet browsers have announced plans to use a unique DNS resolver of their choice as a default. Should these plans be realized, this could mean that internet users will no longer predominantly use DNS servers of their national access provider, but international DNS resolvers predefined by the browser.

The Cologne case was brought in preliminary injunction proceedings. The proceedings on the merits are currently before the first instance court, the District Court (Landgericht) Cologne. This case has the potential to go up even further in proceedings on the merits and it may be that the CJEU has the last word.

---

[1] See for a recent overview: Jan Bernd Nordemann, Website blocking under EU copyright law, in: Rosati, Routledge Handbook of EU Copyright Law, 2021, pages 357 et seq.].

This entry was posted on Monday, July 12th, 2021 at 10:05 am and is filed under Germany, Infringement, Liability
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.