

Cases Wrestle with Role of Online Intermediaries in Fighting Copyright Infringement

June 26, 2012

Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts here:

- [1\) Determining When a Content Host Enjoys Safe Harbor](#)
- [2\) Permissible Obligations for both ISPs and Content Hosts](#)

There have been significant decisions on both sides of the Atlantic in the past several months concerning the legal responsibilities of online intermediaries to police copyright infringement by users.

In the United States, federal appeals court decisions in cases brought against YouTube and Veoh rejected efforts to cripple the "safe harbor" protection that shields user-generated content platforms from monetary liability for infringement committed by users. In Europe, two decisions by the Court of Justice of the European Union (ECJ) appeared to limit the ability of courts to compel intermediaries to filter traffic for infringing content – but recent cases in Germany and the UK took a narrow view of those limits and imposed significant blocking/filtering obligations nonetheless.

Enforcing copyright is a valid and important objective. But enforcement approaches that would saddle online intermediaries with liability for users' infringements or with proactive policing obligations would carry heavy social costs. Safe harbors from liability provide intermediaries such as social networks, photo- and video-sharing sites, blogging platforms, and a wide variety of other tools and services the legal certainty necessary to offer innovative communication services that expand the space for commerce and free expression online. If intermediaries are discouraged from allowing users to post content because of concerns about either liability or the high costs associated with monitoring, preventing, or removing content, then opportunities for speech will be greatly diminished and the full benefits of the Internet will go unrealized.

The role of online intermediaries in controlling copyright infringement is and will likely remain a hotly contested area of law and policy. These recent cases, however, help clarify some important legal parameters. This post will review the impact on key legal issues, first with respect to the applicability of the liability safe harbors for content hosts and then concerning what affirmative obligations courts may impose on both content hosts and ISPs.

- [CDT, *Intermediary Liability: Protecting Internet Platforms for Expression and Innovation* \[1\]](#)
 - [CDT, *Interpreting Grokster: Limits on the Scope of Secondary Liability for Copyright Infringement \(Stanford Technology Law Review 2006\)* \[2\]](#)
-

1. Determining When a Content Host Enjoys Safe Harbor

Both the Digital Millennium Copyright Act (DMCA) in the U.S. and the E-Commerce Directive (ECD) in Europe provide protection for content hosts from monetary liability for third-party content where they lack actual knowledge of infringing activity. Consequently, there has been considerable litigation over what types of hosts qualify for protection, as well as what level of knowledge can disqualify a host. The recent U.S. cases rejected interpretations that would have dramatically limited eligibility for safe harbor protections.

"Active Hosting"

Both the *Viacom v. YouTube* and *UMG v. Shelter Capital Partners (Veoh)* decisions contained good

news regarding the degree to which "active hosts" – services that do more than provide bare-bones content hosting – qualify for protection.

The plaintiffs in each case had aggressively pursued the argument that YouTube and Veoh should not qualify for DMCA protection because their activities went beyond mere hosting. YouTube's efforts to "perform, distribute, and promote stored videos, and to solicit revenues for advertising connected with those videos," Viacom claimed, made YouTube ineligible for protection. UMG argued that Veoh's transcoding of uploaded video files for display went beyond the act of storage protected by the DMCA.

Both courts rejected the idea that the safe harbor is only available for the narrow function of web storage. The ninth circuit, hearing the Veoh case, saw "no basis for adopting UMG's novel theory that Congress intended [the relevant section of the DMCA] to protect only web hosting services." The second circuit likewise rejected almost all of Viacom's arguments, finding that YouTube's related activities (with the possible exception of sublicensing videos to other distributors, an issue remanded to the district court) are closely related to users' initial storage of their videos with YouTube, and therefore fall within the safe harbor. CDT had joined amicus briefs in each case arguing that the video platforms (and other UGC sites) should be protected by the DMCA.

Disallowing protection for platforms that provide services beyond blank-slate hosting would undermine the purposes of the safe harbor by stripping protection from most current and emerging hosting sites. Major sectors of the Internet economy are based on organizing and distributing user-provided content in compelling ways, and these services rely on the legal certainty that safe harbors provide in order to operate. It is therefore encouraging to see U.S. courts make such unequivocal statements about UGC sites' status under the DMCA. The issue is less settled in Europe. Some courts, notably in Italy, have denied protection to services they characterize as "active hosting," which include video-hosting platforms that organize and display users' videos and combine them with advertising. One example is the case against Google Video that resulted in a stunning prison sentence for three Google executives. A July 2011 preliminary ECJ opinion in *L'Oréal v. EBay* arguably may have opened the door to "active hosting" analysis by stating that where an operator has provided assistance which entails optimizing the presentation of offers for sale or promoting those offers, it must be considered as non-neutral and thus ineligible for safe harbor. The recent *SABAM v. Netlog* opinion discussed below expressly held that Netlog qualified as a content host potentially eligible for protection without considering the "active hosting" question, but it appears the Netlog's status as a content host was not contested.

Generalized Knowledge versus Specific Knowledge

Under the U.S. and E.U. frameworks, content hosts can lose liability protection if they have actual knowledge of infringement. Unsurprisingly, exactly what constitutes actual knowledge has been a hotly contested subject of litigation. Both the YouTube and Veoh plaintiffs argued that the video sites knew or should have known, in a general sense, that there was infringing activity on their platforms and that this general knowledge was enough to disqualify them from protection.

Fortunately, both courts soundly rejected that argument. The courts recognized that allowing general knowledge to eliminate safe-harbor protection would render the protection nearly meaningless. Every UGC site, if it operates at any scale, knows at a generalized level that some users inevitably will post infringing content. (Indeed, that is precisely why safe harbor protection is so essential for their ability to operate.) If general knowledge of infringement were enough to forfeit protection, nobody would qualify.

Instead, quoting the Second Circuit opinion, "actual knowledge or awareness of facts or circumstances that indicate specific and identifiable instances of infringement" is required in order to invalidate DMCA protection. The holding is in line with the intent of the DMCA: to allow service providers to build powerful, scalable hosting functions for users without facing crippling liability, while at the same time giving rightsholders a means to address specific infringing content via the notice-and-takedown process. A contrary holding would have gutted the DMCA safe harbor and eliminated protection for countless sites that rely on it.

[UMG v. Shelter Capital \(Veoh\) opinion](#) [3]

[Viacom v. YouTube \[4\] opinion](#) [4]

[CDT amicus brief in Viacom v. YouTube](#) [5]

[CDT amicus brief in UMG v. Veoh](#) [6]

Leslie Harris, "[Deep Impact: Italy's Conviction of Google Execs Threatens Global Internet Freedom](#) [7]," Huffington Post

2. Permissible Obligations for both ISPs and Content Hosts

Mandatory Filtering Disallowed in Europe

Two recent ECJ opinions considered requests by SABAM, a Belgian copyright collecting society, for injunctions ordering an ISP and a social-networking site to install filters to identify and block infringing content. In each case, the court held that mandating filtering would be inconsistent with users' fundamental rights and various EU Directives, including the ECD.

Article 15 of the ECD expressly prohibits Member States from obligating intermediaries to monitor the information they transmit or store, or to seek out indications of illegal activity. The DMCA (at 47 U.S.C. 512(m)) similarly precludes safe harbor from being contingent on an obligation to monitor for infringement. These provisions are essential to the ability of intermediaries to offer robust online services without ongoing, broad-based surveillance features that would jeopardize user privacy and can be expensive if not entirely impractical to operate at Internet scale.

In *SABAM v. Scarlet*, the ECJ rejected an injunction ordering an ISP (a "mere conduit" under the ECD) to filter user traffic so as to identify and block transmissions of songs in SABAM's catalog. The court reasoned that such a mandate:

- constituted a general obligation to monitor traffic (in violation of ECD Article 15);
- was costly and disproportionate (in violation of Article 3 of the Intellectual Property Rights Directive); and
- harmed users' right to personal data protection and right to impart information.

Similarly, in *SABAM v. Netlog*, the ECJ refused to approve a filtering injunction for a social-networking site. Since the proposed filtering mandate would require the site to scan all content its users posted on an ongoing basis in order to ferret out songs from SABAM's catalog, the injunction amounted to a general obligation to monitor prohibited by Article 15.

Clear guidance on this question has been much needed. Over the last few years, there have been several attempts in Europe to impose filtering burdens on UGC platforms. The court of first instance in the *Scarlet* case, for example, had held that the filtering injunction was consistent with Article 15 because the order only applied to specific content (the list of particular musical works supplied by SABAM) and therefore was not a general obligation. In reversing, the ECJ opinion explained the fault with this reasoning: a mandate to filter out a finite list of particular content may be narrower in some respects than a mandate to filter out all infringing content that may be uploaded to the site, but it nonetheless requires scrutinizing all user traffic. It is this type of general monitoring that should be precluded by Article 15, no matter how specific the list of content being filtered.

[SABAM v. Scarlet opinion, ECJ C-70/10](#) [8]

[SABAM v. Netlog \[9\] opinion, ECJ C-360/10](#) [9]

Open Question for Content Hosts: "Notice-and-Stay-Down"

Despite the opinions in the SABAM cases, so-called "notice and stay down" remains an unsettled and troubling issue in Europe. Some courts have imposed duties on content hosts to prevent the reposting of particular content once the service provider has been notified to remove it.

Most recently, a German court ruled in April that YouTube has an obligation to use its Content ID tool to prevent all appearances of videos that include songs about which it receives a takedown notice. In addition, the court ordered YouTube to supplement Content ID with a keyword filter. The court attempted to distinguish its ruling from the *Netlog* case, in reasoning that echoed the lower court in *Scarlet*, by arguing that since the obligation only applied to specific music titles following notice from the rightsholder, it was not general obligation to monitor.

In reality, the notice-and-stay-down requirement imposed by the German court is no different than the obligations rejected in *Scarlet* and *Netlog*. No matter how specific the content being targeted, an obligation to prevent re-uploads means that a service provider must monitor all uploads on an ongoing basis to be sure to catch re-uploads. It is as much an obligation to monitor as the filtering at issue in *Netlog*.

Although the ECD leaves some room for injunctions against intermediaries, notice-and-stay-down also contradicts the purpose of establishing safe harbors in the first place. The German court relied in part on the fact that YouTube already had its Content ID tool to carry out the order, but not all platforms – especially startups – will have the resources to develop sophisticated filtering systems. If new innovators risk having to comply with onerous filtering obligations in order to operate within the safe harbor, they may never get off the ground. And that would undo one of the principal benefits of a liability safe harbor: reducing risk to spur innovation in Internet technologies.

[GEMA v. YouTube judgment, Hamburg District Ct. 310 0 461/10 \(unofficial English translation\)](#) [10]
[DailyMotion v. Zadig Promotions](#) [11], [Cour d'appel de Paris \(in French\)](#) [11]

ISPs Increasingly Subject to Site-Blocking Orders

One final issue that has been increasingly appearing in European courts involves orders for ISPs to block specific sites. Examples are piling up – Grooveshark in the Netherlands, The Pirate Bay in several countries – but two recent decisions in the UK highlight the trend. Courts there have ordered ISPs to block access to The Pirate Bay and Newzbin2, both file-sharing sites found by the courts to facilitate infringement on a massive scale.

UK copyright law, implementing the EU Information Society Directive, allows for blocking injunctions against Internet intermediaries with actual knowledge that their services are being used to infringe copyright. This would seem to be in tension with Article 15 of the ECD, since determining which user transmissions to block arguably requires monitoring all of them. Indeed, British Telecom objected to the first injunction (to block Newzbin2) in part on the basis that it was precluded by Article 15. But the court ruled the injunction permissible:

"The order sought . . . does not require BT to engage in active monitoring . . ., but simply to block (or at least impede) access to the Newzbin2 website by automated means that do not involve detailed inspection of the data of any of BT's subscribers. To the extent that this amounts to monitoring, it is specific rather than general. Furthermore, it would be imposed by a case-specific order made under national legislation which implements Article 8(3) of the Information Society Directive."

This reasoning does little to resolve the legal tension. Forcing an ISP to inspect all web requests and other traffic to see if they are bound for the blocked site certainly results in monitoring of the ISP's general traffic stream. The use of "automated means that do not involve detailed inspection of data" may render it somewhat less onerous or objectionable from a privacy standpoint. But it remains the kind of generally applied monitoring obligation that Article 15 and safe-harbor policies in general have been enacted to prevent.

Beyond the lawyerly parsing of what constitutes a "general" obligation to monitor, ISP blocking carries risks to free expression. Some implementations can be dramatically overbroad, inadvertently blocking more than just the intended site. Moreover, ISP website blocking is a very blunt instrument. Rather than enabling targeted action against specific infringing content, it targets entire platforms,

which may well contain a mix of lawful and infringing content. Issuing blocking orders for such platforms – even those that may have come to be commonly used for infringement – can impair the ability of some users to access lawful expressive material.

There are questions regarding the ultimate effectiveness of ISP blocking as well. A 2010 study by the UK telecom regulator Ofcom noted that "[c]ircumvention of a block is technically a relatively trivial matter irrespective of which of the techniques used."

[Twentieth C. Fox v. BT \(re: Newzbin2\) judgment, 2011 EWHC 1981 \(Ch\)](#) [12]
[Dramatico Entertainment v. British Sky Broadcasting et. al. \[13\] \(re: The Pirate Bay\) judgment, 2012 EWHC 268 \(Ch\)](#) [13]

For more on the policy considerations raised by government-mandated ISP website blocking, see:

[CDT, House testimony, March 2011](#) [14]
[CDT, The Perils of Using the Domain Name System to Address Unlawful Internet Content](#) [15]

Copyright © 2013 by Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL:

<https://cdt.org/policy/cases-wrestle-role-online-intermediaries-fighting-copyright-infringement>

Links:

- [1] https://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_%282010%29.pdf
- [2] <http://stlr.stanford.edu/2006/06/interpreting-grokster/>
- [3] <http://www.ca9.uscourts.gov/datastore/opinions/2011/12/20/09-55902.pdf>
- [4] http://www.ca2.uscourts.gov/decisions/isysquery/95ecf936-a7d2-45fd-a555-e09d3c0e810e/1/doc/10-3270_10-3342_opn.pdf
- [5] https://www.cdt.org/files/pdfs/20110406_google_viacom.pdf
- [6] https://www.cdt.org/files/pdfs/072310_UMG_VEOH_brief.pdf
- [7] http://www.huffingtonpost.com/leslie-harris/deep-impact-italys-convic_b_474648.html
- [8] <http://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=EN&mode=doc&dir=&occ=first&part=1&cid=996022>
- [9] <http://curia.europa.eu/juris/document/document.jsf?text=&docid=119512&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=161927>
- [10] <http://gmriccio.wordpress.com/2012/04/29/hamburg-district-court-gema-v-youtube-english-translation/>
- [11] http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3076
- [12] <http://www.bailii.org/ew/cases/EWHC/Ch/2011/1981.html>
- [13] <http://www.bailii.org/ew/cases/EWHC/Ch/2012/268.html>
- [14] <https://www.cdt.org/testimony/promoting-investment-and-protecting-commerce-online-legitimate-sites-v-parasites-part-i>
- [15] <https://www.cdt.org/report/perils-using-domain-name-system-address-unlawful-internet-content>