Reading the Tea Leaves: ISP Obligations After The Second Circuit's Viacom v. YouTube Decision (2012)

Introduction

Although the Digital Millennium Copyright Act (DMCA) does not require service providers to actively monitor their sites for infringing content, a provider with" knowledge" of infringing activities must act quickly to remove or disable access to these materials. Knowledge comes in two flavors- - actual and imputed - - but after the Second Circuit's decision, ISP obligations related to imputed knowledge are far from clear.

If a provider receives an adequately detailed takedown notice or otherwise acquires actual knowledge of infringing activity, action is required. At least in theory, similar action is required if a provider comes upon facts or circumstances showing apparent infringing activity. To give import to both provisions, it would seem that once an ISP is more than generally aware of apparent infringing activity, it would have a further duty to seek information related to the facts or circumstances showing illicit activity. But is this realistic given the volume of user-generated content on a site like YouTube, as well as the intrinsic difficulty in visually recognizing infringing content? Also, if even with actual knowledge, providers are not obligated to act unless takedown notices describe infringing content with specificity, what is the further duty? With the chance to clarify the parameters of the DMCA, the Second Circuit issued an opaque opinion, from which neither the district court on remand, nor lawyers advising clients, will have an easy job gleaning applicable standards.

The DMCA Safe Harbors

The DMCA provides four safe harbors that, upon service provider satisfaction of certain conditions, immunize the providers from copyright liability. The first safe harbor is for transitory digital network communications; the second for system caching; the third for information residing on systems or networks at the direction of users, and the fourth for search engines. The YouTube case addressed the third (or storage) safe harbor, referencing actions arising "by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider."

The storage safe harbor is conditioned on an ISP's lack of actual or "red flag" knowledge. Upon obtaining either, the provider must promptly remove or disable access to the illicit materials. Further, the ISP may not receive a financial benefit directly attributable to infringing activity, where the provider has the right and ability to control the activity. Although a service provider is not required to affirmatively monitor its service, it must accommodate standard technical measures to identify or protect copyrighted works. Finally, the provider must have a repeat infringer policy and must promptly respond to takedown notices from copyright holders.

The District Court Opinion

The district court opinion was a clean sweep for YouTube. Judge Stanton granted the service provider's summary judgment motion, based on YouTube's lack of knowledge of particular infringements. The court construed both actual and "red flag" knowledge to require item-specific awareness of infringements. Likewise, on the question of YouTube's right and ability to control, the lower court (like the Ninth Circuit in the Veoh case) held that a provider must have item-specific knowledge to control infringing activity. Finally, the district court held that the automated functions that YouTube performs to share videos with users (replication, playback and a related videos feature) are activities performed "by reason of the storage at the direction of a user," within the scope of the storage safe harbor.

The Second Circuit Opinion

On appeal, the Second Circuit agreed with the district court's item-specific standard for both actual and imputed knowledge, but vacated the lower court's decision because a jury could find that YouTube had actual knowledge or awareness of specific infringing activity. Survey evidence showed that 60 to 80% of YouTube's content may have been copyrighted material. More tellingly, YouTube internal emails showed an awareness of particular infringements.

The appellate court also disagreed that the right and ability to control infringing activity should require item-specific knowledge, concluding instead that "something more" than the right and ability to remove or block access to materials, but less than item-specific knowledge, was needed. On remand, the district court will have to determine what that "something more" is.

The right and ability analysis dovetails with the court's introduction of willful blindness into the DMCA calculus. Item-specific knowledge makes sense in the context of the takedown requirement: you can't remove what you don't know about. But notice and takedown are two separate issues. By eliminating the item-specific knowledge shield for the right and ability to control, the court recognizes that it could not have been Congress's intent with the DMCA that a provider could studiously avoid knowledge of what's occurring on its website, while availing itself of safe harbor protection, whether or not it induced infringement. Thus, for now, service providers with a generalized awareness of potential infringements, but lacking specific knowledge, may be open to liability.

Finally, the Second Circuit agreed with the lower court's automated function analysis on three of the YouTube software functions, but remanded for more fact finding on the fourth function -- manual syndication of videos.

Actual Knowledge or "Red Flag" Awareness

Consistent with the Ninth Circuit's Veoh decision, the Second Circuit held that item-specific knowledge is required for both actual and "red flag" knowledge. Logically, if a provider has actual knowledge, it has item-specific knowledge: for example, a YouTube email showing the founders' awareness of the presence on the site of an illicit Bud Light commercial indicates actual knowledge of that item. To justify its item-specific holding, though, the Second Circuit went to great lengths to explain the difference between actual knowledge as a subjective standard, and knowledge of the existence of facts or circumstances as an objective reasonableness standard. So the difference between actual and red flag knowledge is not the difference between specific and general knowledge, but rather between a subjective and an objective standard. Per the court, this reading is also supported by the nature of the removal obligation, since expeditious removal is only possible if a provider knows with particularity which items to remove.

Though it makes sense that item-specific knowledge is required to remove particular infringing materials, the court's analysis essentially reads the "red flag" provision out of the statute. Clearly, once a provider has actual knowledge of the presence of infringing materials, it risks losing its safe harbor protection if it does nothing. It is also clear that Congress contemplated a separate awareness criterion, triggering ISP takedown obligations. But what is item-specific "red flag" knowledge? That the provider knows generally about the likelihood that particular content is infringing? Once there is item-specific awareness, isn't that actual knowledge?

The Second Circuit concluded that although website survey evidence showing a high percentage of infringing content on YouTube site did not establish specific knowledge or awareness of facts or circumstances, several emails produced in discovery identified particular clips and showed YouTube's awareness that the videos were probably infringing. The appellate court vacated the summary judgment on these issues, and remanded to the district court because jurors could find that YouTube had actual or red flag knowledge of these infringements.

Willful Blindness

As a matter of first impression, the appellate court also considered the applicability of the common law concept of willful blindness to the DMCA. But then the appellate court leaves this very appropriate and complex question (without providing a standard) for the district court to resolve. It's curious that this circuit has never addressed this issue before, since Congress assuredly did not want to create the moral hazard of encouraging providers to use as much effort avoiding awareness of infringements as seeking knowledge. So we are left with the question: Should a provider be able to raise the safe harbor defense when it is aware of the high probability of facts in dispute and consciously avoids confirming them? And, if the answer is no, a related question: If the standard for imputed knowledge is item-specific awareness, what knowledge would be imputed – all the facts that a reasonably prudent service provider would have inquired about?

Control and Benefit

The DMCA also mandates that a service provider may not receive a financial benefit directly attributable to infringing activity, where the provider has right and ability to control such activity. The district court had held that the right and ability to control requires item-specific knowledge. The Second Circuit disagreed and remanded for further fact-finding on the issue of control.

The district court had adopted YouTube's construction of the control and benefit provision -- that an ISP must know of a particular instance of infringement before it can control it. However, the Second Circuit reasoned, importing a specific knowledge requirement renders the control provision duplicative, since that provision already excludes from the safe harbor a provider with item-specific knowledge that didn't expeditiously remove an infringing work.

To make things even more difficult for the district court on remand, the Second Circuit also rejected Viacom's construction, holding instead that the control provision does not codify the common law doctrine of vicarious copyright liability (that right and ability coalesce with direct financial interest in the copyrighted materials, even in the absence of actual knowledge). The court's rejection of the Viacom control argument was based on two factors: the DMCA's confusing and unclear legislative history and the illogical effect of the Viacom reading -- since the DMCA requires providers with knowledge to remove or disable access to infringing materials, a provider who removes or disables access would be admitting the right and ability to control and, thus, disqualifying itself from the safe harbor.

Instead, the Second Circuit concluded that the right and ability to control requires something more than the ability to remove or block access to materials posted on a provider's site. It just isn't clear what that "something more" is. The court also held that the right and ability to control does not include a specific knowledge requirement and remanded that issue to the district court to determine whether Viacom had produced sufficient evidence for a jury to conclude that YouTube had the right and ability to control infringing activity and received financial benefit directly attributable to that activity. Without a clear standard, though, it is difficult to anticipate how the district court will resolve this issue.

By Reason of Storage and YouTube's Automated Software Functions

The Second Circuit affirmed the district court regarding YouTube's three automated software functions: conversion (or transcoding) of videos into standard display format; playback of videos on "watch" pages, and the related videos function.

The third safe harbor, the court said, is not limited to merely storing information, like for providers under the first safe harbor. Rather, the storage safe harbor extends to software functions performed for the purpose of facilitating access to user-stored material. Thus,

excluding automated functions like transcoding and playback from safe harbor protections would gut the protections afforded ISPs while hosting user-generated content.

A similar analysis applied to the related video function. Here, YouTube uses an algorithm that identifies and displays thumbnails of clips related to the video selected by a user. The Second Circuit rejected Viacom's argument that the practice promotes rather than provides access to stored content, and is therefore beyond the scope of the safe harbor. Instead, the court concluded that the automated function of indexing and display of related videos retains a sufficient causal link to the prior storage of videos. Further, the related videos function helps YouTube users locate and gain access to material stored at the direction of other users.

Third Party Syndication

A fourth function was not as successful. YouTube manually transcoded a few videos into a format compatible with mobile devices and licensed the videos to Verizon Wireless and some other companies. Viacom argued that these transactions do not occur at the direction of a user. Agreeing, the appellate court remanded the issue for a determination of whether any of the video clips included in the suit were syndicated to third parties.

Repeat infringer policy

The DMCA safe harbor is conditioned on service providers having a policy for termination of repeat infringers. YouTube has a two-tiered system, where it permits partners to gain access to content identification tools. This system was challenged as discriminatory, but the Second Circuit held that although refusing to accommodate or implement a "standard technical measure" exposes a service provider to liability, refusing to provide access to mechanisms by which the ISP monitors its own networks does not vitiate the safe harbor.

Inducement

The district court denied Viacom's summary judgment motion, where it argued for YouTube's liability under a Grokster inducement argument. The Second Circuit broadly concluded that a safe harbor finding immunizes a defendant from all affirmative monetary relief claims, but remanded for further fact-finding on whether YouTube is entitled to the safe harbor.

It has always seemed odd to me that an ISP could induce infringement, yet still argue that it is entitled to safe harbor protection, assuming it has no actual or imputed knowledge of specific infringing activity. Although the Ninth Circuit in Veoh and the YouTube district court concluded otherwise without any analysis, one would think that Congress did not want to encourage infringement by permitting the safe harbor in these circumstances. Presumably, this is where the district court on remand would consider willful blindness, but who knows how that issue will be resolved.

Conclusion

Although a service provider with actual knowledge of infringing site activity has a clear obligation to remove or disable access to the content, its obligations with imputed knowledge are less clear. An ISP has no duty to actively monitor its site, so it is not an investigator in the sense of being a detective. But Congress also included a "red flag" provision in the DMCA, which courts have construed to require ISP takedown once there is item-specific awareness. Assuming that actual knowledge and item-specific awareness are not one and the same, the latter standard must require some provider activity, be it confirmation, validation, investigation, or some similar action.

Yet beyond the vagueness of the imputed knowledge concept and the associated difficulties in turning awareness into actual knowledge are the significant issues associated with investigating the legitimacy of content. This is truly a situation of "I may not know it when I see it." Certainly, service providers are not required to perform rights clearance, but can they even visually determine the legitimacy of materials? Indeed, Viacom had difficulty during the trial identifying its own materials, and there are legion accounts of one part of a media company not knowing that another part has authorized, or even uploaded, allegedly infringing materials. There is a reason there are indemnification clauses in copyright warranties!

Maybe after all of this sound and fury, we are left with only actual knowledge as a workable standard.