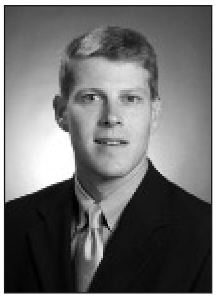
JACK C. SCHECTER

Is it Safe? The Digital Millennium Copyright Act's "Safe Harbor" in the Wake of *Viacom v. YouTube*

In a pivotal scene from the classic film "Marathon Man," the protagonist is interrogated by his nemesis who maddeningly asks over and over again, "Is it safe?"[1] Following the Second Circuit's recent decision in *Viacom v. YouTube*, that same question has been torturing many practitioners who specialize in intellectual property (IP), Internet service providers, and copyright owners as it relates to the "safe harbor" provisions of the Digital Millennium Copyright Act (DMCA).[2]



Happily, unlike the situation faced by our celluloid hero, the answer to this question with respect to the DMCA is relatively straightforward: It is safe. Even though the case was nominally a defeat for defendant, YouTube, the court's decision in *Viacom* has not significantly eroded the safe harbor protections offered by the DMCA.

The Dispute

The fight between media giants Viacom (joined by many other rights holders) on the one side and YouTube and its parent, Google, on the other, centered on Viacom's allegations of copyright infringement based on approximately 79,000 video clips appearing on the YouTube website.

In 2010, a federal judge in Manhattan held that YouTube was entitled to safe harbor protection under the DMCA, because it did not have sufficient knowledge of the copyright infringement occurring on its website.[3] Viacom appealed the decision, and the Second Circuit affirmed in part, vacated in part, reversed in part, and sent the case back to the district court judge.[4]

The Safe Harbor

Even though the DMCA actually provides four separate safe harbors for qualifying Internet service providers (ISPs), the *Viacom v. YouTube* decision is limited to the safe harbor covering copyright infringement claims against ISPs 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."[5] Provided the ISP has met the threshold criteria for eligibility, it is immune from liability under this safe harbor provision if the ISP—

> (A)(i)does not have *actual knowledge* that the material or an activity using the material on the system or network is infringing;
>
> (ii)in the absence of such actual knowledge, is *not aware of facts or circumstances from which infringing activity is apparent*; or
>
> (iii)upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
>
> (B)does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has *the right and ability to control* such activity; and
>
> (C)upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.[6]

Two central issues addressed in *Viacom* concern the extent to which an ISP must be aware of copyright infringement in order for it to lose its safe harbor protection, and what it means for an ISP to have the right and ability to control infringing activity.

Actual and "Red Flag" Knowledge

The Second Circuit considered the difference between actual knowledge of infringement and knowledge of facts or circumstances that make infringement apparent ("red flag knowledge") and rejected Viacom's argument that generalized awareness of infringing activity is sufficient to oust an ISP from the safe harbor. In reaching this conclusion, the court focused on the statutory language, which requires the ISP to expeditiously remove material claimed to be infringing. The court found that, in order to remove infringing material, an ISP would obviously first have to be aware of the specific infringing material.

The court explained that the distinction between actual and red flag knowledge is not one of specific versus generalized knowledge, as Viacom argued, but, rather, between a subjective and objective standard. To have actual knowledge of infringement under the DMCA, an ISP must subjectively know of specific instances of infringement. To have red flag knowledge of infringement, the ISP must be aware of facts that would have made the existence of specific acts of infringement objectively obvious to a reasonable person.

Willful Blindness

The Second Circuit also considered Viacom's argument that an ISP could face liability if it was "willfully blind" to specific infringing activity. Applying a common-law doctrine, Viacom argued that, in a copyright case, a defendant that has taken deliberate efforts to avoid guilty knowledge should not qualify for the safe harbor provisions. After rejecting the notion that the DMCA abrogates this common-law doctrine, the court held that a copyright claimant could cite willful blindness to prove knowledge or awareness of specific instances of infringement. At the same time, the Second Circuit took pains to emphasize that the DMCA does *not* require any affirmative duty on the part of ISPs to monitor their sites for copyright infringement and that willful blindness would have to entail a purposeful avoidance of knowledge of specific instances of infringement.

YouTube's Knowledge of Infringement

Although YouTube prevailed on its central argument that knowledge of infringing activity under the DMCA must be specific rather than generalized, this was not enough to preserve YouTube's win in the lower court.

Surveys conducted for YouTube and Google estimated that as many as 75–80 percent of all YouTube videos at the time contained copyrighted material. The Second Circuit held that such evidence alone was insufficient to create an issue of fact as to whether YouTube had knowledge of specific instances of infringement. So far, so good for YouTube.

On the other hand, YouTube was shown to have contemplated—and decided against—pre-emptively removing "blatantly illegal" unauthorized content, including episodes and clips from specific well-known television programs, commercials, and news broadcasts. The Second Circuit held that these communications could, in fact, support a finding that YouTube had the kind of specific knowledge of infringement that could cost it safe harbor protection.

The Second Circuit concluded that Viacom may have raised material issues of fact regarding YouTube's awareness of specific instances of infringement and remanded the case for further proceedings in the district court.

Right and Ability to Control

The second central question arising from the *Viacom* decision concerns what it means for an ISP to have the "right and ability to control" infringing activity. This question is of critical importance because, under the DMCA, the safe harbor is closed to an ISP receiving a financial benefit from infringing activity when the ISP has the right and ability to control that activity.

YouTube argued that this right and ability to control required that the ISP have item-specific knowledge of infringement. Disagreeing with recent precedent from the Ninth Circuit adopting YouTube's argument, the Second Circuit shot down that position, because it would plainly make the safe harbor requirements regarding knowledge superfluous.

Viacom, for its part, contended that the right and ability to control merely required that the ISP have the ability to block the infringing activity. The court rejected that position as well, because it would render the entire DMCA internally inconsistent, since all ISPs have the ability to block—and are, in fact, required to block—infringing activity upon receipt of a takedown notice from a copyright holder.

In the end, the court simply held that the right and ability to control infringing activity requires "something more" than the ability to remove or block access. But the court passed on the admittedly more difficult question of how to define that "something more."

Instead, the court noted instances of ISPs instituting monitoring programs and providing users with detailed instructions regarding the layout, appearance, and content of their hosted websites. The court suggested that such detailed oversight on the part of an ISP might be an example of the "something more" required to show the right and ability to control. The court added that an ISP's right and ability to control under the DMCA might also be akin to the purposeful, culpable expression and conduct required to show that a party has induced another to commit copyright infringement.

Even though these examples are somewhat helpful, on this question, the Second Circuit avoided an opportunity to provide some much needed clarity and, by and large, punted on this question.

Where Does the Decision Leave Us?

The decision in *Viacom v. YouTube* leaves the state of the law surrounding the safe harbor provision of the DMCA § 512(c) largely untouched.

Of critical importance to ISPs, the Second Circuit reaffirmed that mere generalized awareness of copyright infringement does not remove the protection of the safe harbor, that the DMCA does not require ISPs to affirmatively monitor their sites for infringement, and that the statutory framework does not place the burden on ISPs to determine whether materials are actually illegal.

Even though the court did hold that an ISP might sail outside the DMCA safe harbor by way of willful blindness to infringement, this ruling merely recognizes the common-law doctrine and does not erode

INSIGHT *continued on page 23*

premium. Notwithstanding these rules, employers and employees may negotiate severance provisions where former employees may receive coverage for a period beyond 18 months after termination or where the employer will pay a portion (or all) of the COBRA premium for a specified period of time.

When employers decide to pay for all or a portion of the COBRA premiums, the severance plan must be clear as to how it will affect the former employee's coverage period under COBRA. All too often, severance arrangements are ambiguous when describing how the employer-provided coverage, whether through subsidies or extended coverage, will affect COBRA continuation coverage. For example, a provision that says, "Employer will pay 100 percent of the cost of continued coverage under the Plan for six months" without clear language as to the impact on COBRA continuation coverage is problematic. The former employee may argue that this extended coverage is not part of COBRA and that the 18-month COBRA period begins after the six-month period. If the employer's subsidy is for COBRA coverage, it should be clear in the arrangement that this subsidized coverage is part of and runs concurrently with COBRA.

Occasionally, employers provide continuation coverage extending beyond the 18 months required by COBRA. In these cases, employers who have fully insured plans or stop-loss insurance must contact their providers to make sure such extended continuation coverage is covered under the insurance policy or contract. If the arrangement is not approved by the provider, the employer may find itself self-insuring this extended coverage.

Conclusion

Attorneys have a number of legal compliance issues to consider when drafting severance arrangements. Included among these are employee benefits concerns that must be addressed. The failure to properly account for these issues may result in tax penalties, excise taxes, and/or litigation in unfavorable locations (that is, in state court). By simply identifying, documenting, and clearly describing how compensation and benefits are to be provided under a severance arrangement, employers will be protected from such negative consequences and will provide their attorneys with a number of defenses in litigation should the former employee bring an action related to his or her severance arrangement. **TFL**

Jason Rothman is a shareholder and Aimee Dreiss is an associate in the Employee Benefits Practice Group of Ogletree Deakins. Rothman is based in the firm's Cleveland office, and Dreiss is in the firm's Chicago office.

Endnotes

[1]482 U.S. 1, 18, 19 (1987).

[2]489 U.S. 101 (1989)

[3]Readers should note that this column is intended only to provide a general informational summary of § 409A and is not intended to be relied upon for purposes of determining compliance with that § 409A.

[4]Treas. Reg. § 1.409A-1(b)(1).

[5]Treas. Reg. § 1.409A-1(b)(4).

[6]Treas. Reg. § 1.409A-1(n).

the protection afforded to ISPs under the statute. This is especially so in light of the court's emphasis that, even under a theory of willful blindness, an ISP must be shown to be willfully blind to specific instances of infringement.

Finally, although the Second Circuit failed to clarify the law and created something of a circuit split with the Ninth Circuit, its examples of the "something more" required to constitute the right and ability to control suggest that something *much* more than the ability to block access is required. As long as an Internet service provider is not purposefully and actively inserting itself in dictating the content of the materials of its users, it seems unlikely it would forfeit safe harbor protection by reason of the right and ability to control. **TFL**

Jack C. Schecter is a partner at Sunstein Kann Murphy & Timbers LLP, a boutique firm specialing in intellectual property law in Boston. His practice focuses on litigation, with an emphasis on representing clients in complex patent, trademark, and copyright cases. He is a member of the Federal Bar Association, serving nationally as chair of the Intellectual Property Law Section and locally as a director of the Massachusetts Chapter.

Endnotes

[1]*See* www.youtube.com/watch?v=dG5Qk-jB0D4 (last visited April 25, 2012) for both an example of the type of video clips at issue in the *Viacom* case and the classic referenced scene (be forewarned: the scene is not for the faintheart).

[2]17 U.S.C. § 512.

[3]*See Viacom Int'l Inc. v. YouTube Inc.,* 718 F. Supp. 2d 514 (S.D.N.Y. 2010).

[4]*See Viacom Int'l. Inc. v. YouTube Inc. et al.,* F.3d 2012 WL 1130851 (2d Cir. April 5, 2012).

[5]17 U.S.C. § 512(c).

[6]*Id.* at §§ 512(c)(1)(A), et seq.