Bloomberg BNA

BNA's
Patent, Trademark & Copyright Journal®

COPYRIGHTS

A recent federal court ruling should serve as a wake-up call to ISPs that they need to carefully craft and follow their procedures for responding to allegations of copyright infringement against their users. The ruling doesn't draw clear lines to tell ISPs how to keep their safe harbor protections, but some general guidelines can be gleaned.

What We All Can Learn from BMG v. Cox



BY SIMON J. FRANKEL, MITCHELL A. KAMIN, AND NEEMA T. SAHNI

In what should be a real wake-up call to Internet service providers, late last year a jury sitting in the U.S. District Court for the Eastern District of Virginia found Cox Communications Inc. and a related entity liable for willful contributory copyright infringement.

The jury awarded $25 million in statutory damages to the plaintiff—international music company BMG Rights Management (US) LLC—based on Cox subscribers' use of BitTorrent's peer-to-peer technology to upload and download BMG-copyrighted works.

Simon J. Frankel is a litigation partner at Covington & Burling, San Francisco, where he focuses on copyright and trademark litigation and Internet privacy and technology disputes. Mitchell A. Kamin is a partner at the firm's Los Angeles office, where he focuses on complex civil litigation, white collar and entertainment matters. Neema T. Sahni is a Los Angeles litigation associate; she addresses complex litigation and transactional issues facing clients in the sports, media and entertainment industries.

The verdict followed the district court's rejection of Cox's ''safe harbor'' defense in its decision on summary judgment.[1]

The case has garnered significant industry and press attention as to why Cox, an ISP that simply provides the ''pipes'' for transmitting copyrighted material, was held liable for its subscribers' infringement activity.

Isn't that precisely what Congress intended the safe harbor provisions of the Digital Millennium Copyright Act to prevent?

Here, we examine the district court's decision to deny Cox safe harbor protection. For ISPs seeking such protection, we offer some lessons to be learned in structuring and implementing acceptable use policies—or AUPs—for their users.

And, for rightsholders whose content fills the pipes, we offer a number of takeaways as well.

[1] *BMG Rights Mgmt. (US) LLC v. Cox Commc'ns Inc.*, No. 14-01611, slip op. (E.D. Va. December 1, 2015).

 ISSN 0148-7965

I. The DMCA's Statutory ''Safe Harbors''

In 1998, Congress passed the DMCA[2] to create ''strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment'' while providing ''greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities.''[3] Congress, thus, enacted four statutory ''safe harbors'' that allow ISPs to immunize themselves from liability for the infringing activities of their subscribers where the ISPs' involvement is limited to: (1) transitory digital networking communications; (2) system caching; (3) information residing on ISP systems or networks at the direction of users; or (4) information location tools.[4]

ISPs commonly rely upon the third of these safe harbors, which applies if a user posts infringing material and the ISP, upon notification of claimed infringement, acts expeditiously to take-down the allegedly infringing material—the ''notice-and-takedown'' defense.

In *BMG v. Cox*, however, Cox sought safe-harbor protection under the first safe harbor, claiming it was merely providing transitory digital networking services to its Internet subscribers.

On a motion for summary judgment, Judge Liam O'Grady of the U.S. District Court for the Eastern District of Virginia rejected that defense.

To understand why—and the broader implications of the ruling—we turn to BMG's copyright claims and the policies and procedures Cox had in place to deal with notices of alleged infringement by its subscribers.

II. BMG's Copyright Infringement Claims

BMG holds copyrights in many thousands of musical compositions and, like other owners of protected works, routinely employs Internet-scouring services to search the Internet for potentially infringing uses.

BMG enlisted Rightscorp Inc., which identified instances in which BMG songs were available for download by Cox subscribers, and found that Cox Internet subscribers repeatedly downloaded approximately 1,400 BMG songs using BitTorrent, a P2P file-sharing program.

Rightscorp sent Cox 2.5 million infringement notices, each of which contained an ''offer of settlement.'' Cox, which had a policy to not process infringement notices containing settlement offers, asked Rightscorp to remove that language.

When Rightscorp refused, Cox ''blacklisted'' it, autodeleting incoming Rightscorp emails. Rightscorp then, according to Cox, ''started inundating'' Cox's abuse inbox, so Cox blocked Rightscorp messages altogether.[5] BMG sued for copyright infringement, seeking to hold Cox both contributorily and vicariously liable for the infringing activities of its subscribers.

The parties filed cross-motions for summary judgment on whether the Section 512(a) safe harbor applied.

III. Cox's AUP and Graduated Response Program

Cox's AUP stated that account holders could not use Cox's Internet service to post, copy, transmit or disseminate any content that infringes the copyrights of any party.

It further provided that any violation of the policy terms could result in immediate suspension or termination of a subscriber's service.

To enforce this policy, Cox's abuse department tracked and responded to alleged user infringement activity through the Cox Abuse Tracking System, or ''CATS.''

The court believed three facets of CATS were ''worth mentioning.''[6]

First, when Cox received multiple complaints in a day for a single account, it counted only the first ticket—even if the complaints were for infringement of different works.

Second, Cox imposed a ''hard limit'' on the number of complaints a single complainant could submit in a given day, with a default limit of 200.

Third, Cox defined an abuse cycle as a 180-day period. That meant if—after receiving a complaint for a given account—no complaints were received for that same account within the next six months, the account would be treated as complaint-free.

Like many ISPs, Cox has a ''graduated response program'' to handle and process these notices. With each ''ticket'' received for a particular user, the potential penalties for infringement increase in severity.

In practice, however, Cox would consider termination only after receiving a 14th ticket for a given user. Even then, termination was discretionary.[7]

IV. Denying Cox ''Safe Harbor'' Protection

Cox claimed it fell within the bounds of the Section 512(a) safe harbor (transitory digital networking) because its Internet service did nothing more than ''transmit, route, or provide connections for copyrighted material,'' making it a ''mere conduit'' for the transmissions in question.[8]

To prevail under Section 512, an ISP must demonstrate it has adopted and *reasonably implemented*, and informed subscribers of, a policy that provides for termination in *appropriate circumstances* for subscribers who are *repeat infringers*.[9]

Interpreting this requirement, the court held that, while the DMCA does not impose an affirmative monitoring obligation on ISPs,[10] an ISP is not protected by the safe harbor where there is ''sufficient evidence to create actual knowledge of blatant, repeat infringement by particular users, particularly infringement of a willful and commercial nature,'' and the ISP fails to terminate under such circumstances.[11]

BMG identified three reasons why it believed Cox's repeat infringer policy was not ''reasonably implemented.''

---

[2] Pub. L. No. 105-304, 112 Stat. 2860 (1998)
[3] S. Rep. 105-190, at 20 (1998).
[4] 17 U.S.C. § 512(a)-(d).
[5] *See* Slip Op. at 7.
[6] Slip Op. at 4.
[7] Slip. Op. at 5-6.
[8] Slip Op. at 27.
[9] 17 U.S.C. § 512(i).
[10] *See* Slip Op. at 29.
[11] *Id.* at 30 (quoting *Corbis Corp. v. Amazon.com*, 351 F. Supp. 2d 1090, 1104 (W.D. Wash. 2004)).

  PTCJ ISSN 0148-7965

First, Cox refused to accept and forward the infringement notices it received from Rightscorp because those notices contained settlement offers.

Second, Cox imposed a ''hard limit'' on the number of infringement notices a complainant could submit in a given day.

And *finally*, Cox did not actually terminate access for repeat infringers when warranted.

In denying Cox safe harbor protection, the court relied solely on BMG's third argument, concluding that Cox had failed to terminate subscriber accounts under appropriate circumstances, despite having knowledge of repeat infringement activity.

The court noted that Cox had received DMCA-compliant notices from Rightscorp—''powerful evidence'' of Cox's knowledge.[12]

And the account holders in question had been through all 14 steps of Cox's graduated response procedure, so at that point, ''the chance that the account holder is not a willful infringer has substantially lessened.''[13]

The court next pointed to a series of internal emails in which Cox's manager of customer abuse essentially instructed his team to ignore the DMCA's requirements in dealing with repeat infringers.

The court found these emails evidenced a blatant disregard for the obligations imposed by the DMCA, because ''the immunity granted by Congress to service providers is 'not presumptive' and is to be 'granted only to innocent service providers'. ''[14]

Thus, the emails ''strip Cox of any innocence,'' and ''make clear it was Cox's policy to intentionally circumvent the DMCA.''[15]. The court added that ISPs cannot ''skirt the [DMCA's] termination requirement by imposing something short of complete termination'' of a subscriber account.[16]

Here, Cox was merely suspending and subsequently reactivating repeat infringer accounts, not terminating them. Taken together, the court concluded that Cox could not avail itself of the safe harbors.

On Dec. 17, a jury found that (1) Cox subscribers used Cox's Internet service to infringe BMG copyrighted works, and (2) Cox was liable for contributory infringement—that, with knowledge of alleged infringing activity, it induced, caused or materially contributed to the infringing conduct of its subscribers.

The jury also concluded BMG had proved that Cox's conduct was willful and awarded $25 million to BMG in statutory damages (or roughly $18,000 in damages for each such work).

V. Key Takeaways for ISP-Acceptable Use Policies & Rightsholders Seeking to Protect Copyrighted Works

The discussion of Cox's AUP in light of the allegations made by BMG offers some helpful guidance for ISPs seeking to rely on the DMCA's safe harbor protection. And the *BMG* decision adds to a growing body of case law on the scope of safe harbor protection and the dangers of turning a blind eye to alleged user infringement activity.[17]

A. Graduated Response Procedures

Like many ISPs, Cox handled complaints through a graduated response procedure, which the court does not suggest is per se unreasonable.

But the court *did* suggest the unreasonableness of a program where termination is not considered until a 14th notice is received and, even then, is still discretionary.

Accordingly, the number of steps in an ISP's graduated response program will be relevant to the inquiry of whether that service provider is terminating repeat infringers under ''appropriate circumstances.''

The court did not opine on a magic number of steps, but the opinion strongly suggests that 14 steps are too many, particularly since Cox was not actually adhering to its policy and terminating accounts for which it had received 14 notices.

Although an ISP could certainly argue that a program with 14 steps is reasonable when a termination policy actually is enforced, a smaller number of steps would be more consistent with this ruling.

In any case, the number of notices received before termination is certainly relevant to the question of an ISP's *knowledge* of repeat infringements.

Indeed, in rejecting Cox's claim that it had no knowledge of repeat infringement activity for certain account holders, the court remarked that that could not have been the case where Cox had received not one, not two, but *14* notices of infringement.[18]

So while 14 notices may not necessarily be too many to allow under an AUP, ISPs would be well advised to consider a lower number.

The court's opinion also reaffirms that a service provider's obligation to act is triggered as soon as it has knowledge of repeat infringement activity based on available information.

Accordingly, ISPs should not wait until a user is found liable for infringement before considering termination.

On the other hand, rightsholders seeking to protect their copyrighted works should remain vigilant against repeat infringement activity by sending notices to an ISP *each time* a particular user engages in potential infringement activity.

Indeed, it may take several complaints to an ISP regarding a particular account before the account holder is appropriately penalized under a graduated response program.

Moreover, creating a record of notices sent to the ISP can help establish that the service provider had actual knowledge of the alleged infringement activity and, thus, should not qualify for safe harbor protection.

B. Accurate Recording of Complaints

BMG argued that Cox's refusal to accept and process Rightscorp's notices, and its hard limit on notices from

[12] *Id.* at 41.
[13] *Id.* at 42.
[14] Slip Op. at 35 (quoting *ALS Scan, Inc. v. RemarQ Cmtys., Inc.*, 239 F.3d 619, 625 (4th Cir. 2001)).
[15] *Id.* at 35-36.
[16] *Id.* at 35.
[17] *See, e.g., UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1025 (9th Cir. 2013) (a service provider cannot ''willfully bury its head in the sand'' to avoid obtaining knowledge of infringement activity); *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 31 (2d Cir. 2012) (knowledge or awareness may be established by evidence of willful blindness).
[18] Slip Op. at 41.

a single complainant, made its implementation unreasonable under the DMCA.

The court found it unnecessary to address those arguments, so we are left to guess how they relate to the ''reasonableness'' of Cox's policy.

Still, we *do* know that the court found three features of Cox's abuse tracking system ''worth mentioning'': (1) the ''hard limit,'' (2) the 180-day abuse cycle, and (3) rolling up multiple tickets for a single account in a given day into one ticket.[19]

The summary judgment opinion does not necessarily suggest that Cox's mere unwillingness to accept notices containing settlement offers was itself unreasonable.

Instead, the court seems more troubled by what Cox did next: blacklisting Rightscorp, auto-deleting its messages so information contained therein was never retrieved by Cox, and then blocking the emails altogether at the server level so there is simply no record at all of the messages being received by Cox.

In light of this, ISPs should structure their systems to allow for all notices to be, at a minimum, accepted, recorded and tracked.

Any feature that provides for auto-blocking or ''rolling up'' should be avoided.

While an ISP may have legitimate reasons for not taking any responsive action under certain circumstances, the failure to even record that a notice was received could be deemed unreasonable, as it prevents adequate monitoring of repeat activity and could suggest the service provider is trying to avoid obtaining knowledge that could trigger an obligation or response under its own policy.

For rightsholders, the *BMG* decision could be read to encourage a practice of inundating ISPs with a high volume of infringement notices.

That practice might prompt an ISP to take drastic measures, like those employed by Cox, to delete or block *all* incoming messages which, in turn, might expose the unreasonableness of the ISP's AUP implementation.

Instead, however, it may be more useful for copyright owners to engage directly with ISPs to understand how their tracking systems work, so the rightsholders can send infringement notices in a manner that will actually be recorded and meaningfully addressed by the ISP.

C. Actual Adherence to Established Policies

Perhaps the most obvious takeaway from the court's opinion is that ISPs must actually adhere to the policies they design and implement.

They cannot purport to abide by a termination requirement while, in an effort to hold on to customers in an increasingly competitive market, refusing to terminate customers upon obtaining actual knowledge of repeat infringements.

In other words, once a service provider has proceeded through all preceding steps of its graduated response protocol, it must *actually* terminate the applicable subscriber account, rather than giving the user more chances.

And, as the court made clear, termination has to mean termination. So what is the appropriate duration of termination required?

The opinion suggests that, had Cox actually terminated users under its post-2012 six-month termination policy, it may have qualified for safe harbor protection.

Accordingly, a six-month termination might suffice. However, upon re-activation, giving the user a ''clean slate'' could prove problematic under the court's reasoning.

Therefore, a prudent practice would be for an ISP to retain some notation in the user's restored account, even after the six-month termination period, that the user was previously terminated due to repeat infringement activity.

That information should then be considered if there are more notices of infringing activity as to that user.

Finally, the court seemed concerned with Cox's 180-day ''abuse cycle'' under which a slate was wiped clean after six months of no notices being received on a particular account.

For purposes of structuring an effective graduated response program, ISPs may want to consider tracking notices for longer than 180 days and not ''restarting the clock'' so frequently.

* * *

As noted, the *BMG v. Cox* decision dealt with the Section 512(a) safe harbor for transitory digital networking services—not with the more commonly discussed safe harbor in Section 512(c) for information posted at the direction of users.

Still, while Section 512(c) imposes a different (and lower) bar for ''knowledge'' and other requirements that are not applicable in the Section 512(a) context, many of the lessons from the opinion can have significant implications for ISPs responding to notices of infringing material posted on their systems.

For instance, the decision's acknowledgment that receiving a notice can serve as ''powerful evidence'' of an ISP's knowledge of infringement activity could also be relevant in the Section 512(c) context, as could its reaffirmation that an ISP's obligation to act is triggered before a user is an adjudicated infringer.

Similarly, ISPs will want to take heed of the court's emphasis on the importance of having a reasonable number of steps before termination is considered, actually terminating (rather than suspending) repeat infringer accounts, and tracking and recording all notices received.

Most importantly, as in the Section 512(a) context, ISPs seeking Section 512(c) protection should ensure that their employees follow in practice the policies put in place to comply with the DMCA.

The court's strong rejection of Cox's safe harbor defense, and the substantial jury award for BMG that followed, should serve as a wake-up call for ISPs to reexamine their obligations under the DMCA, their policies, and how closely their practices track their policies.

The decision reminds us that ''safe harbor'' protection is not automatic.

Instead, to qualify for immunity under Section 512, ISPs should structure—and even more critically, follow—their AUPs so as to respond promptly and responsibly to complaints of user infringement activity.

[19] *Id.* at 4.

   ISSN 0148-7965