April 30, 2015

Weil

Alert Intellectual Property/Media

Southern District Ruling Takes Strict Approach to Evaluation of DMCA Repeat Infringer Policy

By Randi W. Singer and Olivia J. Greer

The failure to reasonably implement a repeat infringer policy can disqualify an Internet service provider from safe-harbor immunity from liability for copyright infringement damages under the Digital Millennium Copyright Act (DMCA). Such rulings have been rare, but one cautionary example is the recent ruling in *Capitol Records LLC v. Escape Media Group, Inc.*[1] in the Southern District of New York. On March 25, Judge Alison J. Nathan, adopting in full the report and recommendation of Magistrate Judge Sarah Netburn, ruled that Grooveshark.com, a streaming music service operated by Escape Media Group (Escape), was liable for direct and secondary copyright infringement and was not eligible for a DMCA safe harbor because it failed to terminate users accused repeatedly of uploading infringing works.

In granting summary judgment for plaintiff Capitol Records d/b/a EMI Music (EMI) on all but one count, the court emphasized that Escape's music files were organized in a way that prevented copyright holders from locating infringing content as well as its failure to effectively terminate repeat infringers. The ruling bears careful study by those involved in DMCA compliance for services that host user-generated content.

Background

Escape maintains a central library of sound recordings on its servers. It estimates that 84.5 percent of the recordings in the library belong to major labels with which it has no license.[2] Anyone can search this library and stream music without registering an account. After accepting terms of service on Grooveshark.com, a user can create a free account and submit digital MP3 files to be uploaded to the website's music library. Escape stores a single master copy of each file in its library and streams it to users, who share access to that same file. When uploading a file, users enter certain metadata about the file, including artist, album, and song. After a user uploads a song, Escape's algorithms examine and change the metadata entered by users in order to group MP3 files that appear to contain the same sound recording. Only one file, designated as the "primary file," appears in searches and is streamed to users. The other files containing the same song (the "non-primary files") cannot be streamed or accessed through a search.[3]

Section 512(i) of the DMCA sets forth certain threshold conditions an Internet service provider must meet in order to be eligible for one of four statutory

safe harbors against liability for copyright infringement damages – the most commonly litigated of which is the section 512(c) safe harbor for claims based on material stored on the service provider's system or network at the direction of a user. Section 512(i)(1)(A) provides that a safe harbor is available only if the service provider "has adopted and reasonably implemented, and informs subscribers and account holder of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers."[4]

Escape acknowledged that while its terms of service set out a policy by which users who repeatedly upload infringing files would have their accounts terminated, its practices do not conform to the policy.[5] Rather, Escape follows a "one-strike" policy pursuant to which it disables a user's uploading capabilities after receiving one DMCA-compliant notice of claimed infringement, in addition to removing the file and notifying the user of the actions taken. Escape argued that this policy precludes the possibility of repeat infringers, making it unnecessary for Escape to keep records of infringement complaints or to maintain and implement an actual repeat infringer policy.[6] In addition, when Escape receives a takedown notice that it determines does not meet the precise specifications prescribed by the DMCA,[7] it implements a "DMCA Lite" procedure whereby it removes the identified file but does not notify the user who uploaded the file or revoke the user's uploading privileges.[8]

Escape will process notices of claimed infringement only where a copyright owner identifies the specific web address for the reported song, and web addresses are available only for primary files. The result is what the court described as a "technological Pez dispenser" for infringing music files.[9] For example, if 100 files of a given song reside on Escape's servers, and the copyright owner files a takedown notice, Escape will remove only the primary file, leaving 99 files of the same song on its servers. One of those 99 files would automatically take the place of the removed file, making the song once again available for users to stream. The copyright owner then would have to submit a new takedown notice – 100 takedown notices in all – to actually stop the recording from being streamed on Grooveshark.com. Even then, nothing would prevent the 101st file from being uploaded.[10]

The Grooveshark Ruling

The most notable aspect of the *Grooveshark* ruling is the court's finding that Escape was ineligible for DMCA safe-harbor protection due to its failure to implement a repeat infringer policy.[11] The court found that Escape failed to keep adequate records of infringement; actively prevented copyright owners from collecting information needed to police infringement; and failed to terminate repeat infringers.[12]

The court was particularly troubled by Escape's failure to actually terminate infringing users. The court held that Escape's practice of disabling an infringing user's ability to upload files did not constitute "termination" within the meaning of the DMCA where the user "would still maintain her account and be able to curate her music collection on Grooveshark" and where the infringing user "would be able to search for and stream recordings, as anyone can do without creating an account."[13] According to the court, the "plain meaning" of the DMCA is that an ISP "must, when appropriate, terminate, or 'end,' a subscriber's subscription or an account holder's account," thereby "*disassociat*[ing] themselves fully from repeat infringers, not simply taking measures to impede their infringing activity whole allowing them to maintain [other account privileges]."[14]

The court emphasized that, although the case law has not precisely defined "termination" as used in the DMCA, it was "not aware of any authority for the proposition that something short of complete termination of a repeat infringer's account satisfies 512(i)."[15] The court found that "the plain meaning of the DMCA's language is that, in implementing a repeat infringer policy, the service provider must, when appropriate, terminate, or 'end,' a subscriber's subscription or an account holder's account."[16] To find that Escape's policy of disabling a user's upload

privileges constituted termination would, the court held, "be unprecedented and antithetical to the principle of disassociation and revocation of access that has been expressed by Congress and many courts both in and outside of this district."[17]

Internet service providers would do well to heed this strong language. The court clearly had little patience for policies and practices that smacked of a work-around to allow repeat infringement to continue by "simply tak[ing] measures to impede their infringing activity"[18] rather than terminating repeat infringers. The court also appears to have been exasperated by Escape's failure to comply with the DMCA despite its clear awareness of the safe harbor requirements, as indicated by language in its terms of service stating that it would "terminate a repeat infringer's account and delete all data associated with the account."[19]

The court did acknowledge that courts recognize "a wide range of procedures and practices for implementing a repeat infringer policy that constitute 'implementation' under 512(i)(1)(A)" and stated that they "should continue to do so."[20] This analysis is in line with other courts that have evaluated and accepted policies of graduated consequences for repeat infringers, such as "three strikes" policies, commonly employed by ISPs.[21] However, the ruling is a reminder that in order to ensure compliance with the DMCA, service providers should clearly warn users of possible termination after each instance of infringement; track and actually terminate repeat infringers in "appropriate circumstances"; and immediately terminate users whose sole apparent purpose in using the service is to distribute infringing content.

Conclusion

The district court's ruling in *Escape Media* is not necessarily the last word in the case. The court denied EMI's motion for summary judgment on its claim of direct infringement of its right of reproduction, and a pretrial conference is scheduled for May 11, 2015. If the case settles before trial, this ruling would stand. It is not clear how the Second Circuit would rule on the issues presented if the case were to go up on appeal. In the meantime, the district court has sent a clear warning to ISPs who appear to be hiding the (infringing) ball from copyright owners and failing to actually terminate users who are repeatedly identified as infringers.

1. No. 12-CV-6646(AJN), 2015 WL 1402049 (S.D.N.Y. Mar. 25, 2015).
2. *Id.* at *36.
3. *Id.* at *31-32.
4. 17 U.S.C. § 512(i)(1)(A).
5. *Escape Media*, 2015 WL 1402049, at *48.
6. *Id.* at *32.
7. 17 U.S.C. §512(c)(3)(A)(iii) ("Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.").
8. *Escape Media*, 2015 WL 1402049, at *32.
9. *Id.* at *8.
10. *Id.* at *33.
11. *Id.* at *56.
12. The court found that Escape makes a record only of the infringement by the first user to submit a file; it made no records of any other users who submitted an infringing file subsequently, undermining its argument that its "one strike" policy prevented any repeat infringement. "Due to the importance of adequate recordkeeping to the repeat infringer policy requirement," Escape could not satisfy the DMCA's record keeping requirement. *Id.* at *7. The court also gave great weight to the "technological Pez dispenser" that required rights holders to play "whack-a-mole," *id.* at *8, and made it "all but impossible" to identify and stop the sharing of infringing content. *Id.* at *52.
13. *Id.* at *52 (internal quotations omitted).
14. *Id.* at *53-54 (emphasis in original).
15. *Id.* at *10-11 (citing *Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d. 500, 513 (S.D.N.Y. 2013); *Capitol Records, Inc. v. MP3tunes, LLC*, 821 F. Supp. 2d 627, 638 (S.D.N.Y.2011); *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1101 (W.D.Wash.2004); *In re Aimster Copyright Litig.*, 252 F. Supp. 2d 634, 659 (N.D. Ill. 2002) *aff'd*, 334 F.3d 643 (7th Cir. 2003); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1177-78 (C.D. Cal. 2002)).
16. *Id.* at *53-54.

17. *Id.* at *54.

18. *Id.*

19. *Id.* (internal quotations omitted).

20. *Id.* at *55.

21. *See Disney Enterprises, Inc. v. Hotfile Corp.*, No. 11–20427–CIV, 2013 WL 6336286, at *21 (noting that "the statute does not require Hotfile to maintain a perfect policy (or even anything as stringent as the three-strikes policy it eventually implemented)…"); *Perfect 10, Inc. v. Giganews, Inc.*, 993 F. Supp. 2d 1192, 1197 (C.D. Cal. 2014) (holding a "two-strike" policy of account freezing leading to termination to be reasonably implemented); *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93, 100 (2d Cir. 2010) (in the trademark context, holding a three-strikes repeat infringer policy to be reasonably implemented).

If you have questions concerning the contents of this issue, or would like more information about Weil's IP/Media practice group, please speak to your regular contact at Weil, or to the editors or practice group members listed below:

Editors:

Randi Singer (NY)	Bio Page	randi.singer@weil.com	+1 212 310 8152
Jonathan Bloom (NY)	Bio Page	jonathan.bloom@weil.com	+1 212 310 8775

Contributing Authors:

Randi Singer (NY)	Bio Page	randi.singer@weil.com	+1 212 310 8152
Olivia Greer (NY)	Bio Page	olivia.greer@weil.com	+1 212 310 8815

© 2015 Weil, Gotshal & Manges LLP. All rights reserved. Quotation with attribution is permitted. This publication provides general information and should not be used or taken as legal advice for specific situations that depend on the evaluation of precise factual circumstances. The views expressed in these articles reflect those of the authors and not necessarily the views of Weil, Gotshal & Manges LLP. If you would like to add a colleague to our mailing list, please click here. If you need to change or remove your name from our mailing list, send an email to weil.alerts@weil.com.