

MILRC Media Law Resource Center
MEDIA LAW LETTER

Reporting Developments Through September 30, 2008

LIBEL / PRIVACY

Pa. Super.	Appeals Court Affirms \$3.5 Million Libel Damage Award Against Newspaper <i>Articles About Federal Investigation Were False and Negligently Published</i> Joseph v. Scranton Times	3
7th Cir.	Divided Seventh Circuit Affirms Summary Judgment for Book Author <i>Disputed Recollection of Events Insufficient Evidence of Actual Malice</i> Madison v. Frazier	6
E.D. Okla.	Court Dismisses Suit Against John Grisham, Random House, Other Authors <i>Books about Criminal Proceedings Are "Core Political Speech" Entitled to Highest Protection</i> Peterson et al. v. Grisham, et al	9
S.D.N.Y.	Court Dismisses Defamation and Copyright Claims Against CBS and AP <i>Fair Report Privilege Applied to Foreign Proceeding</i> Idema v. CBS; Idema v. Associated Press	12
Pa. C.P.	Philadelphia Daily News Wins Summary Judgment <i>No Actual Malice; No Defamatory Meaning in Reporting Plaintiff</i> <i>"Appeared as a Playboy centerfold"</i> Miller v. Philadelphia Newspapers	14
Tex. Dist. Ct.	CBS Wins Summary Judgment in Defamation Case <i>Broadcast About Doctor Was Substantially True, Privileged</i> Neely v. CBS	16
NJ	NJ High Court Adds Motive and Speaker Identity Factors for Non-Media Actual Malice <i>Distinguishes Media and Non-media Speakers</i> Senna v. Florimont	18
3rd Cir.	Court Finds NFL Films Violated "Voice of God's" Publicity Right <i>False Endorsement Claim Remanded for Trial on Likelihood of Confusion</i> Facenda v. NFL Films	19
N.Y. Sup. Ct.	Trial Court Dismisses Misappropriation Claim Over Magazine Photo <i>Photograph Bore a Reasonable Relationship to the Article</i> Dominguez v. Vibe Magazine	20
N.J. Sup. Ct.	Suit Against WPIX Dismissed for Failure to Detail Malice <i>Plaintiff Required to Plead Factual Basis of Actual Malice</i> Cats Exclusive Inc. and Jose Pla v. WPIX, Inc., et al.	21
Mont. Dist. Ct.	Montana Jury Awards \$3.2 Million in Libel Suit Against Radio Host <i>Accused Litigation Adversaries of Lying and Fraud</i> Gardner v. Stokes	22

5th Cir.	Court Reverses \$33 Million Defamation Judgment in Physician Peer Review Case <i>Verdict No Longer a Benchmark in Media Cases</i> Poliner v. Texas Health Systems	23
N.H. Sup. Ct.	Trial Court Dismisses Thomas Libel Case After Remand From State Supreme Court <i>Newspaper Protected By Qualified Privilege</i> Thomas v. Telegraph	26
N.J. Sup. Ct.	Venezia Plaintiff Dismisses Case without Payment or Deposition by Reporter Venezia v. North Jersey Media Group Inc.	27
REPORTER'S PRIVILEGE		
E.D. Mich.	Court Rules Reporter Must Reveal Sources in Privacy Act Case <i>Court Rejects Qualified Privilege in Civil Context</i> Convertino v. Department of Justice	28
Mont. Dist. Ct.	Court Quashes Subpoena For Anonymous Posters' Identities On Shield Law Grounds <i>Anonymous Poster's Covered By Shield Law</i> Doty v. Molnar	30
NEWSGATHERING		
Ariz.	Arizona Supreme Court Strengthens Its Rule Allowing Cameras In The Courts <i>New Rule Requires On the Record Findings</i>	31
INTERNATIONAL		
The Netherlands	Supreme Court Allows Monitoring of Journalists "In the Interest of National Security" <i>Leak Investigation Justified Monitoring</i> De Telegraaf Case	32
EMPLOYMENT		
NY	New York State Prohibits Non-Compete Clauses in the Broadcast Industry "Broadcast Employees Freedom to Work Act," (N.Y. Lab. Law § 202-k)	33
COPYRIGHT		
N.D. Cal.	Are There Pirates in My Safe Harbor? <i>ISP Entitled to Safe Harbor Protection for User Generated Content</i> Io Group v. Veoh Networks	34
MLRC		
U. S.	Supreme Court Roundtable on the First Amendment <i>Floyd Abrams, Professor Erwin Chemerinsky & Cliff Sloan on the Direction of the Court on First Amendment Issues</i>	37
Ethics	Joint Defense Agreements In Defamation Litigation – A Primer	43

Are There Pirates in My Safe Harbor?

By Toby Butterfield and Alexis Mueller

The Northern District of California recently granted summary judgment to an internet service provider (“ISP”) whose website permits uploading of user generated content, on the grounds that the ISP had established it was entitled to Safe Harbor protection from liability under §512 of the DMCA. *Io Group, Inc. v. Veoh Networks, Inc.*, No. C06-03926 (N.D. Cal. Aug. 27, 2008) (Lloyd, J.).

The decision is a useful chart for those navigating the digital high seas, and describes what instruments are needed to guide ships of on-line commerce into the DMCA’s Safe Harbor.

Factual Background

The underlying dispute is a copyright claim by Io Group, Inc. (“Io”), a publisher of adult entertainment, against Veoh Networks, Inc. (“Veoh”), the operator of an online video distribution website which provides a means of uploading, sharing and viewing of video clips of varying length. Veoh offers both user-created and user-submitted content, as well as commercially produced videos licensed from sources such as Turner, CBS, US Magazine and Road & Track Magazine.

On cross-motions for summary judgment, the court decided that the safe harbor provision of the Digital Millennium Copyright Act (“DMCA”), 17 U.S.C. § 512(c), protected Veoh from copyright liability for the infringing activity of its users, namely, the unauthorized uploading of ten of Io’s adult video properties.

Qualifying for the DMCA Safe Harbor

To qualify for the safe harbor under § 512(c), an entity must satisfy certain threshold requirements. First, an entity must be a service provider, which is defined as a “provider of online services or network access, or the operator of facilities therefor.” 17 U.S.C. § 512(k)(1)(B). There was no dispute that Veoh met that definition. *Slip Op.* at 12-13.

However, to qualify, the service provider must also adopt and reasonably implement, and inform its users of a policy that provides for the removal of infringing materials and the termination of repeat infringers, as appropriate. 17 U.S.C. § 512(i)(1)

(A). Finally, a service provider must accommodate and not interfere with “standard technical measures” used by copyright owners to identify or protect their copyright works. 17 U.S.C. § 512(i)(1)(B). The DMCA defines “standard technical measures” broadly. 17 U.S.C. § 512(i)(2)(A)-(C).

Io contended that Veoh did not implement its repeat infringer policy reasonably. The court found otherwise, because Veoh had: (a) designated a copyright agent; (b) responded to infringement notices with days; (c) terminated accounts of repeat offenders after one warning and banned the user’s email address; and (d) adopted a means for generating a digital fingerprint for each video file to facilitate with identifying and removing infringing materials and preventing identical files from being uploaded at a later time. *Slip Op.* at 13-14.

Io also contended that Veoh unreasonably did not prevent repeat infringers from reappearing on Veoh’s site under a different user name with a different email address. The court found otherwise, citing the Ninth Circuit’s recent *Perfect 10 v. CCBill* decision that “a service provider need not affirmatively police its users for evidence of repeat infringement.” *Slip Op.* at 14:17-27. Io presented no evidence that any repeat infringer had, in fact, established a new account under a pseudonym, much less that Veoh’s intentionally allowed this to happen. *Id.* 15:13-14.

Finally, Io also argued that Veoh should have tracked users’ identities by IP address. Unpersuaded, the court reiterated that “section 512(i) does not require service providers to track users in a particular way.” *Id.* 16:6-7. Veoh thus qualified for the DMCA safe harbor.

Entering the DMCA Safe Harbor

DMCA § 512(c) limits a qualifying service provider’s liability “for infringement of copyright 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.” 17 U.S.C. § 512(c). However, a qualifying service provider only enters the safe harbor if it designates an agent to receive notices of alleged copyright violations; lacks the requisite knowledge; does not receive a financial benefit from activity it controls; and swiftly removes infringing content. 17 U.S.C. § 512(c)(1)(A)-(C).

(Continued on page 35)

Are There Pirates in My Safe Harbor?

(Continued from page 34)

Io contended that Veoh had not entered the safe harbor because: (a) the infringing materials were not stored on Veoh's system "at the direction of a user"; (b) Veoh was aware of apparent infringement; and (c) Veoh had the right and ability to control the infringing activities and derived a direct financial benefit from such activities.

First, Io contended that the files were not created at the direction of Veoh's users, because Veoh automatically converted any compatible video files uploaded by its users into the Flash format and still image thumbnails. The court disagreed, holding that Veoh did not lose safe harbor protection by automatically processing of user-submitted content, citing the Second Circuit's recent *Cartoon Network v. CSC* decision about who "does" any copying with a complex computer system. *Slip Op.* at 19:19-20 and 20:15-17. See *The Cartoon Network LP v. CSC Holdings, Inc.*, No. 07-1480-cv and 07-1511-cv (2d Cir., Aug. 4, 2008).

Second, Io argued that Veoh was aware of apparent infringing activity (even though Io did not send Veoh a notice and take-down letter before suing) because of the following "red flags": (a) Veoh had constructive notice of Io's copyright registrations; (b) the works in question were apparently professionally created; (c) one of the works contained Io's trademark; and (d) the material did not include the label required of adult video content under 18 U.S.C. § 2257(f)(4).

The court was unconvinced, because: (a) none of the allegedly infringing clips included Io's copyright notice; (b) Io's trademark only appeared several minutes into one clip and no evidence was presented as to Veoh's awareness and willful ignorance of the Io's trademark; (c) there is little to no real world distinction between "professional" and amateur video productions; and (d) the matter before the court did not concern whether there was a violation of 18 U.S.C. § 2257(f)(4).

The court concluded Veoh was not aware of apparently infringing activity and stated that "even assuming Veoh's sufficient knowledge or awareness of the allegedly infringing activity in question, Veoh would not lose safe harbor protection" because it acted expeditiously to remove and disable access to infringing material upon receiving notice thereof. *Slip Op.* at 23:2-4, 23:22-5.

Third, Io contended that Veoh had the "right and ability to control" the infringing activity because it selectively enforced policies that prohibit users from engaging in various types of conduct on its website. However, the court concluded that the

issue is "not whether Veoh has the right and ability to control its system, but rather whether it has the right and ability to control the infringing activity," *Slip Op.* at 24:26-25:1 (emphasis added), and went on to explain that "to escape imposition of vicarious liability, the reserved right to police must be exercised to its fullest extent." *Id.* at 26:20-21 (citing *A&M Records, inc. v. Napster, Inc.*, 239 F.3d 1004, 1023 (9th Cir. 2001) (internal citations omitted)). The court concluded that there was no indication that Veoh failed to police its system "to the fullest extent permitted by its architecture" and that it took steps to reduce, not foster, the incidence of copyright infringement on its website. *Id.* at 29:3-4, 29:15-16.

Finally, Io contended that Veoh should have verified the source of all incoming videos by obtaining the identities and addresses of the submitter and producer and the submitter's authority to upload each file, by hiring more employees or by limiting its website to a smaller number of users and/or files, if necessary. The court disagreed, stating that "the DMCA was intended to facilitate the growth of electronic commerce, not squelch it," and that "Veoh qualifies for safe harbor." *Slip Op.* at 30:17-19.

Analysis

Much has been written and spoken about how the § 512 safe harbor depends on an ISP using "Standard Technical Measures," a term only generally defined by the Act, and which by definition varies over time. This case is therefore another useful ruling on what measures are now "standard." Eliminating repeat offenders is required, but ISPs need not screen for the Internet Protocol address used by alleged repeat offenders. Identifying repeat infringers who use an identical e-mail address is sufficient. This ruling sets a low bar for eliminating repeat offenders, as Hotmail, Yahoo and Gmail all provide multiple free e-mail addresses.

Second, this decision creates an echo of the Second Circuit's recent decision in *Cartoon Network v. CSC*, *supra.*, in which the Second Circuit ruled on whether the owner and operator of a complex computerized system for downloading television programs was a direct infringer when its users selected which files to be copied, stored and later played back. The Second Circuit concluded that only the end user was engaging in a volitional act of copying, not the owner and operator of the service. Likewise in this decision, the Northern District of Cali-

(Continued on page 36)

Are There Pirates in My Safe Harbor?

(Continued from page 35)

fornia has concluded that an ISP “is not precluded from Safe Harbor under § 512(c) by virtue of its automated processing of user-submitted content.” *Slip. Op.* at 19:19-20. The lesson for ISPs is to rely on the computers to do the copying, and not to “actively participate or supervise the uploading of files.” *Id.* at 20:8. The *Veoh* Court even cited *Veoh*’s lack of supervision in concluding that *Veoh* enjoyed safe harbor protection.

Finally, the *Veoh* Court considered the reasonableness of *Veoh*’s actions to remove or disable access to infringing material, and its right and ability to control infringing activity in light of the numerous Ninth Circuit decisions in this area in recent years. The *Veoh* Court distinguished *Napster* as an example of a system created with the sole purpose of providing for “a forum for easy copyright infringement,” and concluded that “there is no indication that *Veoh* has failed to police its system to the fullest extent permitted by its architecture.” *Slip. Op.* at 29:3.

Io’s suggestions that *Veoh* could have improved or changed its business operations to prevent infringing activity did not create a genuine issue of material fact, as “the DMCA does not require service providers to deal with infringers in a particular way.” *Id.* at 30:8.

In its overall analysis, the *Veoh* decision bears some similarities to *Tiffany (NJ) Inc. vs. eBay, Inc.*, 04 Civ. 4607 (RJS)

(S.D.N.Y., July 14, 2008), in which the district court deferred to *eBay*’s decisions about what measures were necessary to prevent infringing material appearing on its website. Like the *Veoh* decision under the DMCA, the *Tiffany* Court subjected *eBay* only to an overall general review of the reasonableness of its measures. Although the *Tiffany* Court was considering trademark liability, not copyright issues or the DMCA, its overall approach is somewhat similar.

However, little analysis has been given, either in this case or in others in this area, to the incentives the law seems

to be creating. The law seems to favor safe harbors for ISPs who have designed a system architecture which fails to prevent infringements so long as an ISP is using its system to the full extent possible. Courts are reluctant to analyze whether the ISP’s system overall is deficient. Perhaps court-appointed experts, such as the expert appointed by the District Court in *Cartoon Network v. CSC*, should provide courts with impartial technical advice, to help them understand the state of the technology in the fast-moving internet technology market.

Toby Butterfield and Alexis Mueller are with Cowan DeBaets Abrahams & Sheppard LLP in New York. Io Group is represented by Gill Sperlein, San Francisco. Veoh is represented by Michael Elkin, Jennifer A. Golinveaux, and Matthew Alex Scherb of Winston & Strawn LLP, San Francisco.

The lesson for ISPs is to rely on the computers to do the copying, and not to “actively participate or supervise the uploading of files.”

NOW AVAILABLE!

**MLRC 50-State Survey:
Employment Libel and Privacy Law 2008**

TOPICS INCLUDE:

- Publication • Compelled Self-Publication • Fault Standards • Damages • Recurring Fact Patterns • Privileges and Defenses • Procedural Issues • Employer Testing of Employees • Searches • Monitoring of Employees • Activities Outside the Workplace
- Records • Negligent Hiring • Intentional Infliction of Emotional Distress • Interference with Economic Advantage • Prima Facie Tort

[Click here to access an order form](#)