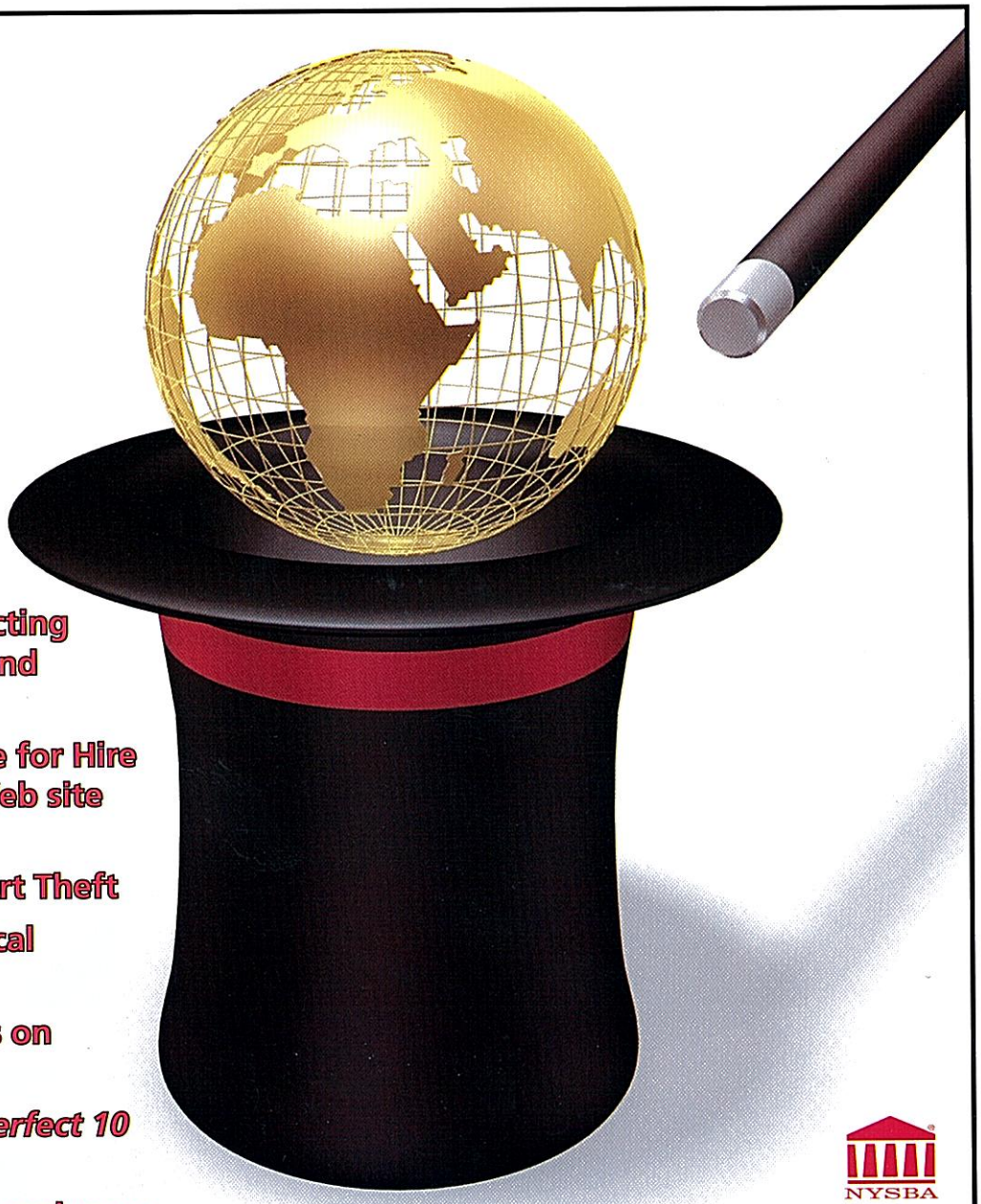
Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=6db24c0d-9e62-44f5-bf37-eab981a0c908

NYSBA FALL/WINTER 2008 | VOL. 19 | NO. 4

Entertainment, Arts and Sports Law Journal

20 YEARS ENTERTAINMENT, ARTS AND SPORTS LAW

A publication of the Entertainment, Arts and Sports Law Section
of the New York State Bar Association



Inside

- 2008 Legislation Affecting Entertainment, Arts and Sports Law
- Applying the Doctrine for Hire and Joint Works to Web site Development
- Conceptual Art and Art Theft
- Compulsory Mechanical Licensing
- Comparative Analysis on PSP Software Cases
- *Tiffany v. eBay*, the *Perfect 10* Cases

. . . and more

NYSBA

Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=6cb24c02-9e63-44f5-bf87-eab991a0c903

Whatever Happened to the "Red Flag" Test?: Knowledge of Infringing Activity On—and the Burden to Police—User-Generated Content Sites After *CCBill, Visa, Io and eBay*

By Frank P. Scibilia and Vanessa Lan

A multitude of Internet sites and services host or store on their servers, and transmit to the public, so-called "user-generated" audio-visual and other content. Most of these sites and services index and/or provide to users the ability to search the content. Most earn revenue from advertising that appears in connection with the content (and some also earn a portion of revenue that the users themselves charge for viewing their so-called "premium content"). Most reformat the content to comply with the site's compression format and some also extract or create thumbnail reproductions or "stills" from the content—arguably implicating the reproduction and derivative works rights.

Of course, a large portion of the so-called "user-generated" content being made available on and via these sites and services was not "generated" by users at all, but rather consists of unlawful reproductions of audiovisual and other material created and/or owned by others with the exclusive right to reproduce, distribute, and create derivative works from that material.

Some of these "user-gen" sites (which include video distribution sites, as well as so-called "social networking sites") have pointed to section 512(c) of the Digital Millennium Copyright Act (DMCA) as a "defense" to claims that they are liable under secondary copyright liability theories for the infringing acts of their end users.[1] They have claimed that the DMCA provides a regime whereby the copyright owners are required to monitor and police the infringing activity on the sites, and provide the sites with notices that list the specific infringing files being exploited on the sites, whereupon the sole responsibility of the site manager is to disable or block access to those specific infringing files (and do no more).[2] These arguments, however, are not consistent with the language of the statute, the legislative history, or the common law upon which the statute was based. Nor do they "encourage responsible behavior and protect important intellectual property rights," two of the goals of the DMCA safe harbor legislation.[3] Rather, they put copyright owners—who are hardly in as good a position to police the Web sites as are the Web sites themselves—in the untenable position of playing a game of "whack a mole," where immediately after a notice of 100 infringing files has been sent to a user-gen service, 200 more infringing files (many mere copies of the files that were the subject of a previously sent notice) appear. The Web sites' pretense that they are in compliance with the DMCA is cynical, given that they are fully aware that the viral nature of their business assures that copyright owners will always be at least one or more steps behind continuing infringing activity.

Knowledge of Infringing Activity

Section 512(c) of the DMCA exempts an online service provider from liability for damages for (and significantly reduces the scope of injunctive relief in connection with) the "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."[4] Yet that so-called "safe harbor" is not available ***unless*** the provider not only "does not have actual knowledge that the material or an activity using the material on [its] system or network is infringing," but also "in the absence of such actual knowledge, ***is not aware of facts or circumstances from which infringing activity is apparent,***" ***and***, "upon obtaining such knowledge ***or awareness***, acts expeditiously to remove, or disable access to, the material."[5] The service provider must, ***in addition***, meet the test of section 512(c)(1)(C), which requires that the service provider, upon being sent a notice that complies with section 512(c)(3) (a DMCA-Compliant Notice), expeditiously remove or disable access to the material that is the subject of the notice.[6] The tests are disjunctive: to benefit from the safe harbor the provider must not have failed to act to remove infringing material in the face of ***either*** actual or constructive knowledge, ***or*** a proper notice.

The legislative history of the section makes plain that Congress did not intend to limit knowledge of infringing activity sufficient to vitiate the safe harbor only to knowledge of specific infringing files to which the provider has been given notice via a DMCA-Compliant Notice. Rather, Congress intended to hold service providers accountable for infringing activity occurring on their sites generally, where that activity would be apparent to a "reasonable person" similarly situated. According to Congress, the knowledge standard "can best be described as a 'red flag' test":[7]

> [I]f the service provider becomes aware of a "red flag" from which infringing

Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=6cb24c0d-9e63-44f5-bf37-eab991a0c903

> activity is apparent, it will lose the limitation of liability if it takes no action. The "red flag" test has both a subjective and an objective element. In determining whether the service provider was aware of a "red flag," the subjective awareness of the service provider of the facts or circumstances in question must be determined. However, in deciding whether those facts or circumstances constitute a "red flag"—in other words, whether infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances—an objective standard should be used.[8]

Failure to act in the face of such a red flag is fatal to the liability limitation, regardless of whether any notice was sent.

> Section 512 does not require use of the notice and take-down procedure. A service provider wishing to benefit from the limitation on liability under subsection (c) must "take down" or disable access to infringing material residing on its system or network of which it has actual knowledge or that meets the "red flag" test, ***even if the copyright owner or its agent does not notify it of a claimed infringement.***[9]

As if that were not clear enough, Congress added: "For their part, copyright owners are not obligated to give notification of claimed infringement in order to enforce their rights."[10]

Section 512(c)'s "red flag" standard is consistent with the common law of contributory and vicarious copyright infringement that forms the basis for the provision.[11] It is also consistent with common sense. To accept the argument that a service need only take action to remove material in response to a DMCA-Compliant Notice—even in the face of rampant and obvious infringing activity taking place on the service—could result in essentially immunizing such a service even if it has actual (albeit general) knowledge that 99 percent of the files on the service are infringing, provided it does not have the requisite "specific" knowledge as to any single file (including where it has deliberately designed its service to avoid obtaining such knowledge, or has otherwise stuck its head in the sand). It would also be a disincentive for services to take commercially reasonable and technologically feasible measures—such as the fingerprinting and filtering measures discussed below—to prevent infringing files from being reproduced and distributed on and via those services. After all, why would a service remove those files that may make up the bulk of its content, or that may be the biggest draw to its service, if it can avoid doing so simply by adhering to a notice-and-[illegible]n regimen?[12]

Quite unfortunately, several recent cases may further embolden such sites and services to continue making the argument that to avoid liability, they need only comply with DMCA-Compliant Notices and take down the specific infringing files listed therein, even where they have knowledge of obviously infringing activity occurring on their sites and the ability to prevent it. These cases water down the "red flag" test that is at the core of the DMCA's liability limitation compromise to the point that it is virtually meaningless, and are in error in that they ignore the clear intent of the statute.

The trend appears to have started in the Ninth Circuit with that Court's decision last year in *Perfect 10, Inc. v. CCBill LLC*.[13] In that case, Perfect 10, an adult Web site, sued CWIE, a provider of Web hosting and related Internet connectivity services, and CCBill, a company that allows consumers to use credit cards or checks to pay for subscriptions or memberships to e-commerce venues, under various secondary copyright liability theories for infringements of Perfect 10's copyrights by customers of CWIW and CCBill.[14] The Ninth Circuit upheld the district court's finding that those entities were entitled to the benefit of the 512(c) safe harbor despite substantial evidence that they were aware of several "red flags" from which infringing activity was apparent.

Perfect 10 had sent numerous notices of infringement to Thomas Fisher, the Executive Vice President of, and the designated agent to receive notices of infringement for, CWIE and CCBill. Perfect 10 also sent Fisher 22,185 pages of screen shots of infringing activity, cross-referenced by name of the Perfect 10 adult model in each infringed photograph.[15] The Ninth Circuit focused on the fact that these notices and screen shots were not DMCA-Compliant Notices, and ignored any role that they may have played in providing CWIE and CCBill with knowledge of infringing activity.[16] The Court stated that the "DMCA notification procedures place the burden of policing copyright infringement—identifying the potentially infringing material and adequately documenting infringement—squarely on the owners of the copyright," and that notice that fails to comply with section 512(c) cannot be deemed to impart awareness "of facts or circumstances from which infringing activity is apparent."[17]

Yet that should not be the case where, as was the case in CCBill, notice (albeit non-DMCA compliant notice) of the infringing activity sufficient to identify, locate and remove or block the infringing material ***was*** provided, and where, ***in addition to such notice***, there were numerous other indicia of infringing activity.[18] Perfect 10 alleged that CWIE and CCBill knowingly provided services to "illegal.net" and "stolencelebritypics.com," and that a disclaimer on "illegal.net" specifically stated that the posted material was copyrighted and that "illegal.net' had no right to them.[19] Perfect 10 further alleged that

CWIE and CCBill knowingly provided services to various password-hacking sites.[20] Yet rather than remand for a determination as to whether a reasonable person, when confronted with Perfect 10's allegations and the screen shots of infringing activity, along with Web addresses with names like "illegal.net" and "stolencelebritypics.com," would have conducted some investigation to determine whether Perfect 10's allegations were true—or even whether CWIE and CCBill actually did conduct such an investigation and discovered infringement but just chose to ignore it and stand on the technicalities of non-compliant DMCA notices—the Court hypothesized various reasons why the existing evidence might not necessarily have made CWIE and CCBill aware of infringing activity. Thus, the Ninth Circuit suggested that the words "illegal" or "stolen" "may be an attempt to increase [the] salacious appeal" of the content on those sites.[21] It noted that the disclaimer on "illegal.net" specifically stated that the Webmaster had the "right to post" the files (even though he admitted that they were copyrighted and he did not claim any right to them).[22] Furthermore, the Court said that passwords on hacking Web sites "could be a hoax, or out of date."[23] In offering up these possible explanations, it completely ignored the objective prong of the "red flag" test, i.e., whether all of those indicia and all of the notices, taken as a whole, would have made infringing activity apparent to a reasonable person operating under the same or similar circumstances as CWIE and CCBill.

The same Ninth Circuit panel that decided *CCBill* strayed even further from the language of the statute and its legislative history in the companion case, *Perfect 10, Inc. v. Visa Int'l Serv. Ass'n*.[24] Employing the classic bootstrap of citing as its only authority its own strained reading of the statute in *CCBill*, the Court there stated, "Congress addressed the issue of notice in the DMCA, which grants a safe harbor against liability to certain service providers, ***even those with actual knowledge of infringement***, if they have not received statutorily compliant notice."[25] This, of course, is not the law, as the statutory test is a disjunctive one, not a conjunctive one, and as the legislative history discussed above makes clear.[26]

In a case decided this summer, *Io Group, Inc. v. Veoh Networks, Inc.*, the Northern District of California struck another blow to the "red flag" test.[27] There, Io, an adult film company, sued Veoh, a user-generated video site, for copyright infringement.[28] The court granted Veoh's motion for summary judgment, concluding that Veoh was eligible for the section 512(c) safe harbor.[29] Io had alleged numerous "red flags," including that it was obvious that the works being uploaded by Veoh users were professionally created, that the uploaded films did not contain certain labels required by law to be placed in adult films (suggesting that the films were not created and uploaded by a legitimate producer of adult films), that one of the infringed films contained Io's trademark several minutes into the clip, that Veoh creates "screencaps" that extract several still images from each file, and that Veoh employees occasionally "spot check" videos after publication.[30] The court nevertheless determined that there was no genuine issue of material fact as to whether Veoh had actual or apparent knowledge of infringement.[31] Citing only an opinion out of the Western District of Washington, the court held that in determining whether a party has apparent knowledge, "the question is not 'what a reasonable person would have deduced given all the circumstances' . . . '[i]nstead the question is whether the service provider deliberately proceeded in the face of blatant factors of which it was aware.'"[32] Thus, like the court in *CCBill*, the *Io* court thereby completely ignored the objective prong of the "red flag" test, which demands that the court determine "whether infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances" as the defendant.[33]

Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=6cb24c0d-9a63-44f5-bf37-eab991a0c903

Outside of the Ninth Circuit, the Southern District of New York's highly publicized decision this past summer in *Tiffany Inc. v. eBay, Inc.* could prove to further muddy the water with respect to the "red flag" test. While *eBay* involved secondary trademark (not copyright) infringement liability, one footnote states: "Under copyright law, generalized knowledge that copyright infringement may take place in an Internet venue is insufficient to impose contributory liability."[34] While that is true as far as it goes—no one is seriously arguing that the fact that a service may know that ***some*** infringement ***may*** take place on its site, without more, gives rise to liability—where there are "red flags" from which infringing activity is apparent, the service must take some action to prevent such activity or it will be liable for it. Thus, the statements in *Tiffany* that the law "demands more specific knowledge as to which items are infringing and which seller is listing those items before requiring eBay to take action" and "does not impose a duty on eBay to take steps in response to generalized knowledge of infringement"[35] should not be distorted to imply that a user-gen service has no duty to take steps to prevent copyright infringement in the face of "red flags," particularly where, as discussed below, it has a right to stop or limit the infringing activity and the practical ability to do so.[36]

The Burden to Police

As noted above, even if the service provider meets each of the three conditions under section 512(c)(1)(A), it must also meet the test of section 512(c)(1)(B), which demands that the service provider "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."[37] "[A] defendant exercises control over a direct infringer when he has both a legal right to stop or limit the directly infringing conduct, as well as the practical ability to do so."[38] Note that there is some degree of overlap between this standard and the section 512(c)(1)(A)/contributory liability standard in that, under the latter, a site can "be held contributorily li-

able if it had knowledge that infringing [files] were available [on the site], could take simple measures to prevent further damage to . . . copyrights, and failed to take such steps."[39]

At least with respect to user-generated content sites, this raises the issue of the extent to which those sites should be required to police and stop or limit the distribution of infringing files using fingerprinting and filtering technologies.[40]

The court in *Io* noted that Veoh had "adopted means for generating a digital 'fingerprint' for each video file which enables Veoh to terminate access to any other identical files from ever being uploaded by any user."[41] In fact, it pointed to Veoh's fingerprinting as evidence that Veoh was policing its system "to the fullest extent permitted by its architecture," stating that "[o]nce content has been identified as infringing, Veoh's digital fingerprinting technology also prevents the same infringing content from ever being uploaded again."[42] The court did not, however, discuss under what circumstances content on Veoh was "identified as infringing" such that Veoh employed the fingerprinting technology. One might presume that it did so with respect to content as to which it received a DMCA-Compliant Notice, but the court did not go so far as to require Veoh to employ the technology to prevent the upload of all files that matched those named in a DMCA-Compliant Notice. For that reason, as well as the court's apparent reluctance to require Veoh to take steps in response to objective "red flag" criteria, it seems unlikely that at least that court would require that a service that had such technology use it to prevent any reasonably apparent infringing activity from recurring (that is, require the fingerprinting, filtering and blocking of "red flag" files).

Nevertheless, given the cost of infringement to copyright owners, the potential profitability of user-generated content sites, and the relatively low cost and widespread availability of content fingerprinting/filtering solutions, the authors would posit that all user-generated services should be required to implement such a solution "to stop or limit the directly infringing conduct."[43] Such sites should employ the solution to fingerprint all files listed in a DMCA-Compliant Notice, as well as all "red flag" files. For example, the site should use the solution to "disable access to infringing material residing on its system or network of which it has actual knowledge or that meets the 'red flag' test, even if the copyright owner or its agent does not notify it of a claimed infringement."[44]

In fact, these solutions can aid in policing infringement, i.e., in locating and pre-emptively excluding infringing materials. Content owners can provide digital files (including, where relevant, audio or video files) of all of the copyrighted content they wish to prevent from being uploaded to and distributed via the service; the service can create fingerprints of all of those files and can then (1) search for and remove or block all "legacy" files on the service matching those fingerprints, and (2) prevent files matching such fingerprints from being uploaded.

Digital Fingerprinting from JDSUPRA in
https://www.jdsupra.com/post/documentViewer.aspx?fid=6cb24c0d-9e63-44f5-bf37-eab991a0c903

To require the implementation and use of such solutions is consistent with the Ninth Circuit in *Amazon* remanding Perfect 10's contributory infringement claim to the district court to resolve the "factual disputes over whether there are reasonable and feasible means for Google to refrain from providing access to infringing images,"[45] as well as its conclusion that "without image-recognition technology, Google lacks the practical ability to police the infringing activities of third-party websites."[46] It is consistent with Judge Patel's modified preliminary injunction in *Napster*—upheld by the Ninth Circuit—ordering the Napster system to be shut down until Napster implemented a "non-text-based filtering mechanism."[47] It is also consistent with the Central District of California's holding in *Tur v. YouTube* that, with respect to user-generated sites, the "right and ability to control" prong of the section 512(c)(1)(B)/vicarious liability standard "presupposes some antecedent ability to limit or filter copyrighted material."[48]

In fact, it is even consistent with the decision in *eBay*, although that decision, again, contains some unfortunate language that will no doubt be distorted by those who wish to limit or even eliminate the burden on Web services to police their premises and prevent infringing activity (and do nothing other than respond to DMCA-Compliant Notices, which does not solve the problem and is not the outer limit of such services' obligation to prevent infringement). There, the court was highly focused on "who should bear the burden of policing Tiffany's valuable trademarks in Internet commerce."[49] The court concluded that "rights holders bear the principal responsibility to police their trademarks," even if eBay were better situated "to staunch the tide of trademark infringement."[50]

The facts of *eBay*, however, bear no resemblance to infringement of copyrights in digital files reproduced and distributed on or via user-generated content sites. The *eBay* court focused heavily on eBay's use of its "fraud engine," which identified "blatant instances of potentially infringing or otherwise problematic activity,"[51] as well as its VeRO Program.[52] Yet neither the fraud engine nor the VeRO Program—nor any other solution that eBay could have created—could determine whether a listed item was actually counterfeit. That determination could only be made by physically inspecting the particular piece of jewelry at issue, and the jewelry was never in the hands of eBay. On the other hand, a copy of each potentially infringing file ***exists on the user-generated content site***. It is, in effect, in the site's possession, and a filtering solution can determine whether such a file is actually infringing. It can be matched against fingerprinted files of copyrighted content that is not authorized for distribution on the service.

Conclusion

These cases might merely be examples of the ancient axiom that hard cases make bad law. After all, the *CCBill* and *Visa* cases pitted an adult Web site against credit card and payment services; the plaintiff in the *Io* case was also a purveyor of adult content. This might explain the cursory way in which the courts in both *Visa* and *Io* distinguished the defendants in those cases from Napster on the ground that in *Napster*, "the sole purpose of the Napster program was to provide a forum for easy copyright infringement."[53] Yet as Judge Kozinsky correctly noted in his *Visa* dissent, "*Napster* and *Grokster* are not the endpoint of this court's caselaw: Even though Google has many legitimate, noninfringing uses, *Amazon* held that it would be guilty of contributory infringement if it could modify its service to avoid helping infringers."[54]

Unfortunately, the holdings of these cases could lead to absurd results. Taken to their logical extreme, they could immunize the provision of obviously infringing material such as bootlegged copies of movies in current theatrical release with file names such as bootleggedcopyofthedarkknight.mpeg or justrippedcopyofporkandbeansbyweezer.mp3. As Professor Nimmer noted, in discussing *CCBill*, "[w]ith the eponymously named 'illegal' ruled inadequate to raise a red flag of illegality, it is difficult to imagine just how crimson one would have to be in order to qualify."[55] Moreover, to the extent these holdings incorrectly convert section 512(c) into a mere notice-and-take-down statute, and place the brunt of policing infringement on the copyright owners, they could also disincentivize those Web sites with the ability to prevent or limit infringement from taking commercially reasonable and technologically practical measures to do so, such as using fingerprinting technology to take down all infringing legacy content on the site of which it has actual knowledge or that meets the "red flag" test, and to prevent such content from ever again being uploaded.

Endnotes

1. *See, e.g., Io Group, Inc. v. Veoh Networks, Inc.*, No. C06-03926 (HRL), 2008 WL 4065872 (N.D.Cal. August 27, 2008); *Tur v. YouTube, Inc.*, No. CV064436 (FMC) (AJWX), 2007 WL 1893635 (C.D.Cal. June 20, 2007). The DMCA does not limit liability for direct infringements by these services, such as the infringements that may occur in connection with or as the result of the formatting, indexing, and extracting functions described above. *See, e.g.*, H.R. Rep. 105-551 (II), at 53 (1998); S. Rep. 105-190, at 43 (1998) ("Information that resides on the system or network operated by or for the service provider through its own acts or decisions and not at the direction of a user does not fall within the liability limitation of subsection (c)."). As the *Io* decision demonstrates, determining whether the information resides on the system through the provider's acts or at the direction of a user is not always an easy task.
2. *See, e.g.*, The Electronic Frontier Foundation's "Fair Use Principles for User Generated Video Content," *available at* http://www.eff.org/issues/ip-and-free-speech/fair-use-principles-usergen.
3. *See, e.g.*, Statements on Introduced Bills and Joint Resolutions on S. 2037, Statement of Mr. Leahy (May 6, 1998).
4. 17 U.S.C. § 512(c).
5. 17 U.S.C. § 512(c)(1)(A)(i)-(iii) (emphasis added). Even if service provider meets each of the three conditions under that section, it must ***also*** meet the test of section 512(c)(1)(B), which demands that the service provider "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." 17 U.S.C. § 512(c)(1)(B).
6. 17 U.S.C. § 512(c)(1)(C).
7. S. Rep. 105-190, at 44; H.R. Rep. 105-551 (II), at 53.
8. *Id.*
9. S. Rep. 105-190, at 45; H.R. Rep. 105-551 (II), at 54 (emphasis added).
10. *Id.*
11. *See, e.g., Ellison v. Robertson*, 357 F.3d 1072, 1077 (9th Cir. 2004) (finding AOL liable for contributory infringement when it changed its contact e-mail address and missed e-mails noticing copyright infringement, since "a reasonable trier of fact could find that AOL had reason to know of potentially infringing activity"); *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 261 (9th Cir. 1996) (finding swap meet operator contributorily liable for sale of counterfeit tapes by its vendors after it received letters from the sheriff imparting generalized knowledge that infringing goods were being sold at its meet); *Microsoft Corp. v. EEE Bus. Inc.*, 555 F. Supp. 2d 1051, 1059 (N.D. Cal. 2008) (stating, "[a]n individual may be liable for contributory infringement even where she does not have actual knowledge of the infringing activity, but should have reason to know of the infringing conduct"); *Arista Records, Inc. v. Flea World, Inc.*, No. 03-2670 (JBS), 2006 WL 842883 at *14 (D.N.J. Mar. 31, 2006) (finding defendants incorrect in their proposition that knowledge of "specific infringements" is necessary for contributory infringement, since this argument runs contrary to past case law); *Playboy Enters., Inc. v. Russ Hardenburgh, Inc.*, 982 F. Supp. 503, 514 (N.D. Ohio 1997) (finding computer bulletin board service contributorily liable where it had "at least constructive knowledge that infringing activity was likely to be occurring"); *Sega Enters. Ltd. v. Maphia*, 857 F. Supp. 679, 686–87 (N.D. Cal. 1994) (finding bulletin board service operator contributorily liable even though it did "not know exactly when [copyrighted] games will be uploaded to or downloaded from" its service); *A&M Records, Inc. v. General Audio Video* Cassettes, 948 F. Supp. 1449, 1457-58 (C.D. Cal. 1996) ("[a]lthough there is no direct evidence that [defendant] knew he was contributing to the illegal copying of each of these 156 different sound recordings, the testimony at trial indicated that [he] was aware that he was contributing to the counterfeiting of many different sound recordings"); *RSO Records v. Peri*, 596 F. Supp. 849, 858 (S.D.N.Y. 1984) (finding knowledge of infringing use where "the very nature of color separation manufacture—the photographing of the packaging of copyrighted records and tapes—would suggest infringement to a rational person").
12. Indeed, in the *Napster* case, an internal memorandum produced in discovery revealed that Napster recognized that forcing copyright owners to send DMCA-Compliant Notices in order to enforce their rights would be "a seriously onerous task" which "would have little or no effect" on Napster (or the infringing activity occurring thereon). *A&M Records, Inc. v. Napster, Inc.*, Nos 00-16401 and 00-16403 (9th Cir. Sept. 8, 2000), Brief of Plaintiffs/Appellees at 36, available at 2000 WL 34018835.
13. 488 F.3d 1102 (9th Cir. 2007).
14. *Id.* at 1108.
15. *Id.* at 1112.
16. *Id.* at 1112–13.
17. *Id.* at 1113, 1114.
18. *See* S. Rep. 105-190, at 45; H.R. Rep. 105-551 (II), at 54 (service provider wishing to benefit from the limitation on liability under subsection (c) must 'take down' or disable access to infringing material residing on its system or network of which it has actual

Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=6ab24c0d-9a63-44f5-bf37-eeb901a0c903

knowledge or that meets the 'red flag' test, even if the copyright owner or its agent does not notify it of a claimed infringement").

19. *Id.* at 1114.
20. *Id.*
21. *Id.*
22. *Id.*
23. *Id.* Professor Nimmer characterizes the court's ruling in *CCBill* as "that the [red] flag's fabric must essentially whip against the face of the party to be bound (and probably raise a few welts in the process)." 3 M. & D. NIMMER, NIMMER ON COPYRIGHT [hereinafter, "NIMMER"] § 12B.05[C][1] (2008). Indeed, by substituting its own hypotheses at the dispositive motion stage for a trial as to what CCBill actually knew about, or what a reasonable person in CCBill's position should have recognized was infringing activity, it effectively foreclosed any determination that any such "whipping" or "welting" had actually occurred.
24. 494 F.3d 788 (9th Cir. 2007).
25. *Id.* at 795 n. 4 (emphasis added).
26. *See* notes 8-11 and accompanying text.
27. *Io Group, Inc. v. Veoh Networks, Inc.*, No. C06-03926 (HRL), 2008 WL 4065872 (N.D. Cal. August 27, 2008).
28. *Id.*
29. *Id.* at * 20.
30. *Id.* at *14.
31. *Id.* at *13-15.
32. *Id.* at 14 (quoting *Corbis Corp. v. Amazon.com, Inc.*, 351 F.Supp.2d 1090, 1108 (W.D. Wash. 2004)).
33. S. Rep. 105-190, at 44; H.R. Rep. 105-551 (II), at 53. Note that Io did not send Veoh any notices of infringement, DMCA-compliant or otherwise, but proceeded straight to filing a complaint. Still, given the holding in *CCBill*, it is doubtful that sending non-compliant notices would have changed the *Io* court's holding. On the other hand, given the volume of traffic on user-gen sites like Veoh, it is doubtful that even sending DMCA-Compliant Notices would have solved Io's infringement problem. *See* n. 13, *supra.*
34. *Tiffany (NJ) Inc. v. eBay, Inc.*, No. 04 Civ. 4607 (RJS), 2008 WL 2755787, at n. 37 (S.D.N.Y. July 14, 2008).
35. *Id.* at *1, 43.
36. The Court in *eBay* noted that eBay had a business interest in common with Tiffany in assuring that "knock-offs" of trademarked products not be sold on its site. *Id.* at * 1. That commonality of interest appears a great deal less apparent with respect to Web sites purveying unlicensed copyrighted content.
37. 17 U.S.C. § 512(c)(1)(B).
38. *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146,1173 (9th Cir. 2007), quoting *MGM Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 930 (2005).
39. *Id.* at 1172.
40. For a description of digital video fingerprinting, see hhtp://en.wikipedia.org/wiki/Digital_video_fingerprinting. For a description of digital audio fingerprinting, see http://en.wikipedia.org/wiki/Audio_fingerprinting.

Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=6cb24c0d-9e63-44f5-bf37-eab991a0c903

41. 2008 WL 4065872, at *3.
42. *Id.* at *19. Moreover, it was clear that Veoh was able to police its site and prevent certain files from being distributed when it wanted to, given that Veoh had, by the time the suit was filed, and on its own volition, terminated access to all adult content. *Id.* at *2.
43. 508 F.3d at 1172 (9th Cir. 2007), quoting *MGM, Inc. v. Grokster, Ltd.*, 545 U.S. at 930.
44. S. Rep. 105-190, at 45; H.R. Rep. 105-551 (II), at 54 (emphasis added).
45. 508 F.3d 1146 at 1172–73.
46. *Id.* at 1174.
47. *A&M Records, Inc. v. Napster, Inc.*, 284 F.3d 1091, 1097–98 (9th Cir. 2002). The injunction also required Napster to "continually search [its] index and block all files" that contained a work as to which Napster was given notice of infringement. *Id.* at 1096. *See also Napster, Inc.*, 239 F.3d at 1027 (holding that Napster must "affirmatively use its ability to patrol its system and preclude access to potentially infringing files listed in its search index").
48. 2007 WL 1893635, at *3.
49. *Tiffany*, 2008 WL 2755787, at *1.
50. *Id.* at *47.
51. *Id.* at *8.
52. *Id.* at *9–10.
53. *Visa*, 494 F.3d at 799 n. 5; *Io*, 2008 WL 4065872, at *18.
54. 494 F.3d at 811 n. 4 (Kozinsky, J., dissenting).
55. NIMMER § 12B.05[C][1].

Frank Scibilia is a partner in the interdisciplinary New Media Group at Pryor Cashman LLP in New York, specializing in transactions and litigation in emerging media, particularly the digital distribution of copyrighted audio and visual content. He has negotiated and drafted agreements licensing catalogs of musical compositions and sound and audio-visual recordings for distribution on and via user-generated video sites, lawful peer-to-peer services, interactive streaming services, advertiser-supported services, and other emerging media platforms. He has also been involved in some of the most significant litigation in this area (including in the *Napster, Aimster, Grokster, MP3.com*, and *Multiply.com* cases), as well as in rate-setting and the crafting of proposed legislation in this arena.

Vanessa Lan is an associate in the litigation department at Pryor Cashman.

Get CLE Credit:
Write for the *EASL Journal*!