To: Geoff Brigham
From: Andrew Alire
Re: Summary of *UMG v. Veoh*

Veoh, a "service provider" under the Digital Millennium Copyright Act (DMCA), is a web service that allows users to upload and share videos with other users, both through its website and through a stand-alone software client. Some of these videos are copyrighted. Based on this practice, Universal Music Group (UMG), a large music publishing company, brought suit in district court against Veoh for direct, vicarious, and contributory copyright infringement, as well as for inducement of infringement.[1] The district court found that Veoh was protected by the DMCA's safe harbor provision[2] and dismissed UMG's complaint on summary judgment.

On appeal, UMG made three arguments for reversing the district court's decision. The Ninth Circuit rejected each argument and affirmed the decision of the district court. UMG's arguments are presented below, in the order that the court addressed them. A short explanation of that argument and why the court rejected it follows. A summary of the court's holdings is provided last.

1) UMG argued that alleged infringing activities do not fall within the plain meaning of "infringement of copyright by reason of the storage [of material] at the direction of a user," a threshold requirement under § 512(c)(1).

Veoh, upon receiving a video submission by a user, would commence an automated pre-storage process[3] designed to facilitate sharing on its network. UMG argued that under this process, the alleged infringement occurred not *by reason of* the "storage of material" but, rather, *by reason of* the "access that the storage facilitates," thus disqualifying it from safe harbor protection. Op. at *16. UMG also argued that this process did not occur "at the direction of a user," as defined by § 521(c).

The court rejected this claim by first finding that UMG's construction of "by reason of" was too narrow. UMG had argued that similar language had been narrowly interpreted in other statutes (*i.e.*, RICO and the Clayton Act), but the court reasoned that here, under the DMCA, this language should be broadly interpreted; both as a matter of policy and because the interpretation urged by UMG would create internal statutory conflicts within the DMCA itself.

---

[1] UMG argued that the DMCA's safe harbor provision did not apply, despite the fact that (1) Veoh had complied with all DMCA takedown requests, (2) that it could not prove Veoh ever failed to takedown copyrighted materials it became aware of by other means, and (3) that Veoh had implemented various procedures to prevent copyright infringement on its network. The court emphasized these procedures, which included retaining a third party which used "audio fingerprints" to assist with identifying infringing videos that had been uploaded. Upon identifying an infringing video, Veoh also utilized its own "hash filtering" technology to automatically disable access to any identical videos and block any subsequently submitted duplicates. These measures resulted in the removal of over 60,000 videos from Veoh and the termination of thousands of user accounts identified as repeat violators. Op. at *9-10.

[2] § 512(c)(1) limits the liability of service providers for infringement of copyright by reason of the storage [of material], on their system or network, at the direction of a user.

[3] "When a video is uploaded, various automated processes take place. Veoh's software automatically breaks down the video file into smaller 256-kilobyte "chunks," which facilitate making the video accessible to others. Veoh's software also automatically converts, or "transcodes," the video file into Flash 7 format. This is done because "the vast majority of internet users have software that can play videos" in this format. Veoh presets the requisite settings for the Flash conversion. If the user is a "Pro" user, Veoh's software also converts the uploaded video into Flash 8 and MPEG-4 formats, which are playable on some portable devices. Accordingly, when a Pro user uploads a video, Veoh automatically creates and retains four copies: the chunked file, the Flash 7 file, the Flash 8 file and the MPEG-4 file. None of these automated conversions affects the content of the video." Op. at *8.

The court also rejected UMG's argument that this process did not take place at the "direction of a user" by pointing out that Congress had *expected* "service providers" to "modify user-submitted material to facilitate storage and access, as Veoh's automatic processes do." Op. at *22. Thus, UMG's argument that this process contravened user direction made little sense

2) UMG argued that genuine issues of fact remain about whether Veoh had actual knowledge of infringement under § 512(c)(1)(A)(i), or it was aware of facts or circumstances from which infringing activity was apparent under § 512(c)(1)(A)(ii).

UMG argued here that it should have been allowed to prove that Veoh had "sufficient knowledge of infringement,"[4] or at least an awareness of apparent infringement (*i.e.*, an awareness of "red flags"),[5] by showing that Veoh "must have known" the shared content was unauthorized "given its general knowledge that its services could be used to post infringing material." Op. at *24.

The court rejected the first argument, finding that the "actual knowledge" standard could not be met by a showing of only "constructive knowledge" (*i.e.*, what UMG called "sufficient knowledge"). The court, guided by the principle that the burden of policing copyright infringement rests on the copyright holder, held instead that *specific* knowledge was required under the statute, and that Veoh had removed all infringing content that it had *specific* knowledge of.

The court was similarly unpersuaded by UMG's attempt to prove Veoh's awareness of "red flags" by demonstrating it had "general knowledge" of the existence of infringing material on its network. Reasoning again from the premise that the burden of proving infringement rests with the copyright holder, the court held that more than a generalized knowledge of infringing activity was required. Lastly, the court rejected even what it described as UMG's strongest argument: that Veoh was aware of *specific* infringing activity identified in *e-mails* sent to it by certain copyright holders. The court, no doubt sensing an attempted end-run around the DMCA's notice and takedown provision,[6] held here that copyright holders could not prove Veoh's awareness of red flags by pointing to notice made outside of the provisions set forth therein.[7]

3) UMG argued that it presented sufficient evidence that Veoh received a financial benefit directly attributable to infringing activity" that Veoh had the right and ability to control under § 512(c)(1)(B).

Pointing to Veoh's general ability to search for, identify, and remove infringing videos, UMG argued that Veoh had the "right and ability" to control infringing activity, and so was exempt from the protection of the safe harbor provision. The court rejected this argument, holding instead that the "the right and ability to control" under § 512(c) means control over *specific infringing activity* the provider knows about. Op. at *35. It went on to state that a "service provider's general right and ability to remove materials from its services is, alone, insufficient." *Id*.

---

[4] § 512(c)(1)(A)(i).

[5] § 512(c)(1)(A)(ii). The term "red flags" is taken from *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1114 (9th Cir. 2007).

[6] § 501(c)(3).

[7] The court did leave open the possibility of proving the awareness of "red flags" where notice from *non-copyright holders* was made outside of the DMCA's procedures, however. Op. at *31.

The Law After *Veoh*

The holdings of this case are as follows:

- A service provider's automated formatting of user-submitted media, prior to storage on its network, does not negate the application of the DMCA's safe harbor provision if such processes are intended to facilitate sharing on that provider's network. Op. at *22-23.

- Proving that a service provider had "actual knowledge" of the existence of infringing material on its network, pursuant to § 512(c)(1)(A)(i), requires a showing of "specific knowledge" as to the location of that infringing material. "Constructive" or "general" knowledge will not suffice. Op. at *27

- Proving that a service provider was "aware of facts or circumstances from which infringing activity is apparent," pursuant to § 512(c)(1)(A)(ii), requires more than a showing that it had "general knowledge" of the the existence of infringing activity on its network. Op. at *27-28. However, what constitutes more than a general knowledge, but less than specific knowledge, remains unclear.

- Copyright holders may not create "actual knowledge" of infringing material under § 512(c)(1)(A)(i), or the "aware[ness] of facts or circumstances from which infringing activity is apparent" under § 512(c)(1)(A)(ii), by noticing infringement to a service provider in a manner that does not comply the DMCA's notice and takedown provisions under § 501(c)(3). Op. at *30-31

- A service providers "right and ability to control," as defined by § 512(c), requires control over specific infringing activity the provider knows about. A service provider's general right and ability to remove materials from its services is, alone, insufficient. Op. at *35. This appears to apply the same definition of "actual knowledge" as used in § 512(c)(1)(A)(i).