

HEINONLINE

Citation: 59 J. Copyright Soc'y U.S.A. 627 2011-2012



Content downloaded/printed from
HeinOnline (<http://heinonline.org>)
Sat Nov 14 21:18:54 2015

- Your use of this HeinOnline PDF indicates your acceptance of HeinOnline's Terms and Conditions of the license agreement available at <http://heinonline.org/HOL/License>
- The search text of this PDF is generated from uncorrected OCR text.
- To obtain permission to use this article beyond the scope of your HeinOnline license, please use:

[https://www.copyright.com/ccc/basicSearch.do?
&operation=go&searchType=0
&lastSearch=simple&all=on&titleOrStdNo=0886-3520](https://www.copyright.com/ccc/basicSearch.do?&operation=go&searchType=0&lastSearch=simple&all=on&titleOrStdNo=0886-3520)

COPYRIGHT ENFORCEMENT AND ONLINE FILE HOSTING SERVICES: HAVE COURTS STRUCK THE PROPER BALANCE?

by MARY RASENBERGER AND CHRISTINE PEPE*

I. INTRODUCTION	628
II. CAN FILE HOSTING SERVICES BE HELD DIRECTLY LIABLE FOR COYRIGHT INFRINGEMENT?	631
A. The Volitional Conduct Requirement and the Rise of Netcom Immunity	632
B. Under the Transmit Clause: Public or “Private” Performance?	638
C. The Import of the Cases: Establishing Direct Infringement in the Context of File Hosting Services ..	643
III. SECONDARY LIABILITY AND THE DMCA	646
A. Contributory Infringement	647
1. Material Contribution: Providing the Site and Facilities for Infringement.....	647
2. Material Contribution: Ability to Prevent Further Damage but Failure to Do So	650
3. Sony Test: Supplying a Product that is Used to Infringe	651
4. Willful Blindness as Knowledge	651
5. <i>Grokster</i> Test: Actively Encouraging or Inducing Infringement	652
B. Vicarious Liability	658
C. Section 512(c) Safe Harbor Protection	661
1. Do File Hosting Services Fall Within Section 512(c)?	662
2. Section 512(c) Requirements.....	666

*Mary Rasenberger is a partner at the law firm of Cowan, DeBaets, Abrahams and Sheppard, LLP. Christine Pepe is the Assistant Vice President of Legal Affairs at the American Society of Composers, Authors and Publishers (ASCAP). The views expressed in this article are solely those of the authors. The authors thank Jenette Wiser, J.D., Pace University Law School 2012, and Erin Watkins, J.D. Fordham University School of Law 2013, for their research assistance.

3. <i>Post-Viacom v. YouTube and UMG Recordings v. Shelter Capital: The Import of the Recent Section 512 Cases</i>	686
IV. CONCLUSION	692

I. INTRODUCTION

Business models for the digital distribution of entertainment content are shifting rapidly, with the overarching goal of providing users anywhere, anytime access to as much content as possible. Various types of file hosting services, including various forms of so-called “locker” services and user-generated content Web sites, have grown in availability and popularity, revolutionizing how consumers store, access and share content.¹

Apple, Google and Amazon offer “cloud” or “locker” services that allow users to access their personal music, video, photo and document libraries on virtually any device.² Movie studios are getting into the locker game — a consortium of studios and consumer electronics companies has created a cloud-based service known as UltraViolet. UltraViolet gives users a “digital locker” that stores copies of movies they purchased on DVD or Blue-ray and allows them to watch these films anywhere, anytime.

Cyberlocker services, also referred to as “one-click hosting” sites, such as Hotfile, RapidShare, 4Shared, MediaFire and the recently shut-down Megaupload, have been growing in availability in the last couple of years. These services allow users to upload files from their computers so that they might be shared with anyone in the world. Generally, the user is given a Uniform Resource Locator (URL) for each file uploaded and may share that URL link with anyone. Most file hosting services do not secure these URLs unless the user specifically marks the file as “private.” As such, the files are often searchable and retrievable by the public through indexes provided by the service itself or third parties.³ While these services

¹ As used in this article, a file hosting service generally refers to any service that hosts user files and allows users to store and access content using the provider's servers. File hosting services include “cyberlocker” and “cloud” services, as well services that facilitate access to user-generated or user-posted content, whether video, image or audio. File hosting services often permit file sharing, but can be distinguished from the peer-to-peer and Bit Torrent file sharing models.

² Although certain music-based cloud services are offered by well-known companies such as Apple, Google and Amazon, questions remain whether all required licenses have been obtained for these services, and that issue is not the focus of this article.

³ In the wake of the Megaupload indictment, MediaFire, which does not index its own site and sets non-indexable meta tags, blocked access to FilesTube, a service which had been crawling and indexing files on the MediaFire ser-

are used to share personal photos with friends and family, store personal music and movie libraries for access from multiple devices, or to send documents to colleagues, some of these file hosting services target and reward the same type of illegal file sharing as peer-to-peer file sharing services. For instance, through file hosting services, users may upload infringing copies of copyrighted content for others to download and may themselves also download numerous infringing copies. Such services may also reward customers who upload popular content that is frequently downloaded by others since the more popular the content, the more traffic and advertising revenue the service generates.⁴ And while their policies may be neutral as to whether the content is infringing, the vast majority of content made available through some of these file hosting services reportedly consists of unauthorized copyrighted content.⁵

Certain cyberlocker services may also be used by copyright pirates as a means of providing unauthorized distribution or performances to users, who may or may not be charged for the privilege of accessing copyrighted content. Many pirate sites currently provide streaming or downloads to their users by providing links back to the cyberlocker service. An example of a service used for this type of service is Megaupload, whose founders were arrested and whose site was shut down by the U.S. Department of Justice as part of an alleged \$175 million criminal copyright infringement conspiracy.

User-generated content (“UGC”) sites, often used more as user-posted content sites (meaning users post third-party copyrighted content

vice. *Mediafire Starts Blocking FileTube Search Traffic*, TORRENTFREAK (Apr. 22, 2012), <http://torrentfreak.com/mediafire-starts-blocking-filetube-links-1220422>.

⁴ Recently, RapidShare published an anti-piracy policy containing guidelines on how responsible cyberlocker and cloud hosting sites should conduct their business going forward to reduce infringement. RapidShare stated that, unlike other file hosting sites, it maintains no incentive programs to reward users for the number of times their files are downloaded and has also reduced download speeds to deter pirates. See, e.g., *RapidShare Overtures Snubbed, “Must Do Better” Say Labels*, TORRENTFREAK (Apr. 21, 2012), <http://torrentfreak.com/rapidshare-overtures-snubbed-must-do-better-say-labels-120421>.

⁵ See *Cyberlockers Take over File-Sharing Lead from Bittorent Sites*, TORRENTFREAK (Jan. 11, 2011), <http://torrentfreak.com/cyberlockers-take-over-sharing-lead-from-bittorent-sites-110111> (“Megaupload, Hotfile, 4Shared, Mediafire and RapidShare are all listed in the top 100 most visited sites on the Internet before The Pirate Bay, and newcomers such as Fileserve are eager to do the same. It is worth noting and exemplary of the growing trend that half of these sites are younger than two years. In a report (pdf) published by MarkMonitor today it is concluded that RapidShare is the leading ‘digital piracy’ site with over 13 billion yearly visitors, followed by Megaupload with close to 5 billion visits.”).

rather than their own creations), have also grown in availability and popularity. As do the cyberlocker services, these sites similarly allow users to upload copyrighted content and make it available to the world (or a group of so-called “friends”) without authorization. Some examples of this type of service are YouTube, Veoh, Facebook and Pinterest.

In theory, it would seem that certain file hosting services that encourage or facilitate infringement and profit from the infringement should have some potential liability for copyright infringement, either directly, or secondarily under theories of inducement, contributory or vicarious liability. However, as discussed below, in practice it has proved challenging to hold these services responsible for infringement occurring on their sites, even if they have knowingly profited from the infringement. Due to the way courts have construed direct and secondary liability in the online context, combined with the manner in which they have interpreted the safe harbors under the Digital Millennium Copyright Act (“DMCA”), copyright owners face multiple obstacles in enforcing their rights against all types of file hosting services. While U.S. courts have found many unauthorized peer-to-peer file sharing sites liable for contributory and/or vicarious infringement, the new generation of file hosting services, whether so-called “cloud” or “locker” services or UGC and user-posted sites, by and large have not been found liable to date.

While the business model shift to cloud and other types file hosting services has numerous benefits for online consumers and technology companies, the potential impact of the massive amounts of infringement allowed by, and in some cases even encouraged by, these services on creators and their authorized distributors is a serious issue. Already the revenue of the music, motion picture, newspaper and book publishing industries has substantially declined, while technology company revenues continue to soar.⁶

In this article, we: (1) review the trend in the case law away from imposing any direct or secondary liability on file hosting service providers, or any obligation for them to cooperate with rights holders other than through DMCA notice and takedown procedures, (2) examine how file hosting services that encourage infringement are generally escaping liability, while peer-to-peer services generally have not, and (3) analyze whether interpretation of the law in recent cases has achieved the right balance between protecting copyright and encouraging innovation. We

⁶ ROBERT LEVINE, *FREE RIDE: HOW DIGITAL PARASITES ARE DESTROYING THE CULTURE BUSINESS, AND HOW THE CULTURE BUSINESS CAN FIGHT BACK*, 1-3 (2011); *see also* David Waterman & Sung Wook Ji, *Online v. Offline in the U.S.: Are the Media Shrinking?* 12-13 (rev. Nov. 18, 2011), *available at* http://www.indiana.edu/~telecom/people/faculty/waterman/Online-Offline_Working%20paper-Nov.pdf.

question whether certain decisions have perhaps gone too far in protecting service providers to protect the growth of the Internet, an already robust, profitable industry, to the serious detriment of creators and copyright owners by making it difficult for them to enforce and profit from their copyrights.⁷

Copyright protections are meaningless if they cannot be enforced. From the individual creator to the major industry player, many are losing their ability to effectively exercise their copyright rights and profit from the works they create and/or distribute simply because they cannot enforce those rights. They are seeing their profits diverted to service providers who pay nothing for the ability to host and make copyrighted content available. We note that now might be a good time to reevaluate, and possibly, recalibrate, how the courts have interpreted the responsibilities of the growing numbers of file hosting services to cooperate with copyright owners if, as a nation, we are concerned about protecting one of our greatest natural resources — our creativity. It is a simple equation: if our creators cannot enforce their basic rights online, there will be less creativity.

II. CAN FILE HOSTING SERVICES BE HELD DIRECTLY LIABLE FOR COPYRIGHT INFRINGEMENT?

Copyright owners could potentially assert claims for direct copyright infringement against file hosting services that store and provide access to massive quantities of infringing content. The claim would be that the service provider itself is displaying, reproducing, distributing or, for example, in cases where access to audiovisual or audio works is provided via streaming transmissions, publicly performing the copyrighted content without authorization.⁸ While a user may push or click on the button to cause the

⁷ As Levine notes, the inherent conflict lies in the fact that the online companies that have built businesses upon other people's creative content are not the entities that funded the creation of the content in the first place. He states, technology start-ups like Grooveshark and Hotfile are still building businesses on the same model: users share content illegally while the company that allows them to do so profits. This doesn't only hurt creators whose work is taken without payment; it harms the entire online economy. Who wants to build a legitimate music business when it's easier to start an illegal one? Why would anyone invest in a staff of reporters and editors when it's so much cheaper to aggregate the work of others? How can any company compete with a rival that offers its products but bears none of the expenses? The free ride has become the road to riches.

LEVINE, *supra* note 6, at 8.

⁸ Under what is known as the "transmit clause" of the Copyright Act, to perform or display a work "publicly" means to "transmit or otherwise communicate a performance or display of the work . . . to the public, by means of any device or process, whether the members of the public capable of receiv-

copy to be made or uploaded or to initiate the transmission, it is the services' systems that actually make and upload the copies and transmit or stream the content to the recipient. Below, we discuss the important cases that impact whether a file hosting service could be held directly liable for copyright infringement.

A. *The Volitional Conduct Requirement and the Rise of Netcom Immunity*

Although copyright is a strict liability statute, courts have cautioned that for direct infringement to be found there must be some element of volition or direct causation on the part of the accused infringer. Therefore, beginning in the mid-1990s, in the context of Internet bulletin board services (BBS) and prior to the DMCA, a body of cases developed that attempted to delineate when an "Internet service provider" (ISP) could be said to have sufficient volition to be directly liable for copyright infringement.⁹ *Religious Technology Center v. Netcom On-Line Communication Services, Inc., et al. ("Netcom")*¹⁰ established what has, in large part, become the standard for direct liability volition in online cases. The plaintiffs in *Netcom* sued both the bulletin board service and the ISP, Netcom, for the unauthorized reproduction and public distribution and display of the works of Scientology's L. Ron Hubbard.¹¹ Netcom was an ISP in the traditional sense, providing general Internet access much as Verizon and Time Warner Cable do today.¹² In declining to find direct infringement by Netcom, the district court stated: "Netcom's act of designing or implementing a system that automatically and uniformly creates temporary copies of all data sent through it is not unlike that of the owner of a copying machine who lets the public make copies with it."¹³ The court further compared Netcom to a phone company and concluded that Netcom was

ing the performance or display receive it in the same place or in separate places and at the same time or at different times." 17 U.S.C. § 101 (2006).

⁹ Prominent during the late 1970s through the mid-1990s, the online BBS, or Bulletin Board System, was one of the first identifiable digital file hosting models. Once logged into the BBS, users could upload and download data, read bulletins, and exchange messages with other users on the message boards. As MP3 files spread on the Internet, the BBS was largely supplanted by peer-to-peer file sharing networks, e.g., Napster, Gnutella, and Kazaa, and ultimately the BitTorrent file sharing model. Currently, as described above, cyberlockers, such as Hotfile, RapidShare, Megaupload, are the most prominent online file hosting model.

¹⁰ 907 F. Supp. 1361 (N.D. Cal. 1995).

¹¹ *Id.* at 1368.

¹² *Id.*

¹³ *Id.* at 1369.

merely a “passive conduit for information”¹⁴ and should not be held liable for merely “setting up and operating a system that is necessary for the functioning of the Internet.”¹⁵ Using similar reasoning, the court declined to find the bulletin board operator directly liable.¹⁶ The *Netcom* court concluded: “Only the subscriber should be liable for causing the distribution of plaintiffs’ work, as the contributing actions of the BBS provider are automatic and indiscriminate.”¹⁷

Subsequent to *Netcom*, however, two district court cases found sufficient volition to impose direct liability on the service operators. In *Playboy Enterprises v. Russ Hardenburgh, Inc.*, a district court found direct infringement of the distribution and display rights by the bulletin board service based on the fact that the service encouraged users to upload files and also utilized a screening process.¹⁸ These facts, the court reasoned, transformed the defendant from “passive providers of a space in which infringing activities happened to active participants in the process of copyright infringement.”¹⁹ In another case brought by Playboy, *Playboy Enterprises, Inc. v. Webbworld, Inc.*, a district court found direct infringement of the reproduction, distribution and display right by the service provider Webbworld, rejecting the argument that it was a “mere conduit between its subscribers and adult-oriented newsgroups.”²⁰ Webbworld would receive news feeds from certain adult-oriented Internet newsgroups, where users posted or uploaded articles consisting of text and images.²¹ Upon receipt of this newsfeed, Webbworld, using its own proprietary “ScanNews” software, would retain the sexually-oriented images (creating two thumbnails of each image) and thereafter, offer both the full-sized and thumbnail images to its paying subscribers.²² In distinguishing Webbworld from the defendants in *Netcom*, the court stated: “Webbworld functioned primarily as a store, a commercial destination within the Internet. Just as a merchant might re-package and sell merchandise from a wholesaler, so did Webbworld re-package (by deleting text and creating thumbnails) and sell images it obtained from the various newsgroups.”²³ Importantly, the court emphasized Webbworld’s total dominion over the control of its site and the product it offered to its clientele, concluding:

¹⁴ *Id.* at 1370 n.12.

¹⁵ *Id.* at 1372.

¹⁶ *Id.* at 1370-71.

¹⁷ *Id.* at 1372 (citing *Playboy Enters., Inc. v. Frena*, 839 F. Supp. 1552, 1554 (M.D. Fla. 1993)).

¹⁸ 982 F. Supp. 503, 513 (N.D. Ohio 1997).

¹⁹ *Id.*

²⁰ 991 F. Supp. 543, 552 (N.D. Tex. 1997).

²¹ *Id.* at 549-50.

²² *Id.*

²³ *Id.* at 552,

As a shop owner may choose from what sources he or she contracts to buy merchandise, so, too, did Webworld have the ability to choose its newsgroup sources. Clearly, a newsgroup named, for example, "alt.sexy.playboy" or "alt.mag.playboy" might instantly be perceived as problematic from the standpoint of federal copyright law.²⁴

After the DMCA had been enacted, the Fourth Circuit in *Costar Group, Inc. v. LoopNet, Inc.* further expanded *Netcom* immunity to a Web site operator that allowed its real estate broker subscribers to post listings and photos, many of which were copyrighted.²⁵ LoopNet's service focused on real estate listings — it was not a general provider of Internet access or even a general BBS. Nonetheless, the Fourth Circuit compared LoopNet to Netcom, holding that LoopNet's conduct was passive, as it was LoopNet's subscribers who uploaded the photos and therefore engaged in the volitional conduct.²⁶ The dissenting opinion attempted to distinguish LoopNet from Netcom on the basis that LoopNet had a policy of pre-approving all photos on its Web site and screening photos to ensure they were in the proper format.²⁷ Relying on *Russ Hardenburgh*, the dissent argued that any type of screening process or involvement transformed LoopNet from a passive provider of access into an active participant in the process of copyright infringement.²⁸

In 2008, in *Cartoon Network LLP v. CSC Holdings, Inc.* (referred to as "*Cablevision*"), the Second Circuit extended *Netcom* immunity to a cable operator by holding that Cablevision could not be held directly liable for the copies made by subscribers to Cablevision's Remote Storage Digital Video Recorder ("RS-DVR") system.²⁹ Relying on *Netcom* and *CoStar Group*, the Second Circuit reversed the district court's finding of direct liability (by stipulation, no secondary liability claims were asserted).³⁰ The Second Circuit held that because Cablevision's customers

²⁴ *Id.* at 552-53. But see *infra* Section III.3.b(i) for discussion of *Perfect 10, Inc. v. CCBill, LLC*, 488 F.3d 1102 (9th Cir. 2007) (the fact that defendants provided services to sites entitled "illegal.net" and "stolencelebritypic.com" did not constitute red flag awareness under the DMCA).

²⁵ 373 F.3d 544, 546-47 (4th Cir. 2004).

²⁶ *Id.* at 547.

²⁷ *Id.* at 557.

²⁸ *Id.* at 558 (citing *Playboy Enters., Inc. v. Russ Hardenburgh, Inc.*, 982 F. Supp. 503, 513 (N.D. Ohio 1997)).

²⁹ 536 F.3d 121, 130-33 (2d Cir. 2008).

³⁰ *Id.* The district court rejected application of *Netcom* and Cablevision's efforts to paint itself as entirely passive in the RS-DVR recording process. *Twentieth Century Fox Film Corp. v. Cablevision Sys. Corp.*, 478 F. Supp. 2d 607, 618-620 (S.D.N.Y. 2007). The district court did not view the RS-DVR system as simply a stand-alone piece of equipment akin to a VCR or copy machine, as Cablevision argued, but instead analogized it to VOD (video-on-demand), noting that Cablevision actually provided the content being

issue the record command directly to the system, which then automatically obeys such commands and engages in no volitional conduct, Cablevision resembles a store proprietor who charges customers to use a photocopier on his premises.³¹ It seems incorrect, reasoned the court, to say that such a proprietor makes any copies when his machines are operated by his customers.³² In overruling the lower court's rationale, the Second Circuit stated: "We do not believe that an RS-DVR customer is sufficiently distinguishable from a VCR user to impose liability as a direct infringer on a different party for copies that are made automatically upon that customer's command."³³

The Second Circuit in *Cablevision* also rejected defendants' parallel volitional argument with regard to the public performance right, i.e., that there was no direct infringement of the public performance right because the customer, not Cablevision, initiated playback of the recorded content and therefore "performed" or "transmitted" the copyrighted content.³⁴ In declining to extend *Netcom* to the public performance right, the court concluded that "the definitions that delineate the contours of the reproduction and public performance rights vary in significant ways."³⁵ Ultimately, however, based on the unique copy transmission theory, discussed below, the court held that all transmissions were private and that Cablevision did not infringe the public performance right.

copied, maintained the service on its own premises and maintained a continuing relationship with its customers. *Id.* The district court viewed Cablevision's involvement in the recording process sufficient enough to conclude that it "would be 'doing' the copying, notwithstanding that the copying would be done at the customer's behest." *Id.* at 620.

³¹ *Cartoon Network*, 536 F.3d at 131.

³² *Id.* According to the Second Circuit, this type of scenario stands in stark contrast to where a request is made to a human employee, who then volitionally operates the copying system to make the copies for the customer, as was the case in *Princeton University Press*, where the defendant was found directly liable. *Id.* (citing *Princeton Univ. Press v. Michigan Document Servs.*, 99 F.3d 1381, 1383 (6th Cir. 1996) (en banc)). In *Princeton University Press*, the defendant operated a commercial copy shop that reproduced, bound and sold substantial segments of copyrighted content as course packs to students. *Princeton University Press*, 99 F.3d at 1383.

³³ *Cartoon Network*, 536 F.3d at 131. The Second Circuit viewed the facts relied upon by the district court as relevant to contributory — not direct — infringement and intimated that a stronger case for plaintiffs could have been presented if secondary copyright infringement had in fact been asserted. Many of the facts relied upon by the district court distinguished the Cablevision case from the *Sony* case, where secondary infringement was not found based on the sale of the VCR device. *Id.* at 132-33 (citing *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 437-38 (1984)).

³⁴ *Cartoon Network*, 536 F.3d at 134.

³⁵ *Id.*

In 2009, the district court in *Arista Records, LLC v. Usenet.com, Inc.* rejected the application of *Netcom*, *Costar Group* and *Cablevision*, and instead held the service provider directly liable for infringing the distribution right.³⁶ This type of direct liability ruling against an ISP, which seems increasingly rare given judicial predilection for applying *Netcom*, followed the older, pre-DMCA *Russ Hardenburgh* and *Webbworld* line of cases.³⁷ In *Arista v. Usenet*, the Usenet service operated as a file distribution service that made copyrighted music available for users to download.³⁸ Defendant Usenet argued that it operated akin to a “common carrier” that delivers requested content to subscribers automatically without active involvement.³⁹ The court disagreed and found sufficient volition based on the fact that Usenet took active measures to create servers dedicated to MP3 files and to increase retention times of newsgroups containing MP3 files, and further engaged in filtering of content.⁴⁰

Judicial predilection for *Netcom* immunity appeared again in the more recent *Disney Enterprises, Inc. v. Hotfile Corp.* case, where a Florida district court extended *Netcom* immunity to Hotfile, a true file hosting service.⁴¹ Hotfile makes copies of each file uploaded by its users and creates a URL link for each, from which any user can then download the file.⁴² Disney argued that because Hotfile’s servers automatically made five additional copies of every file uploaded by a user (and then assigned a unique link to each copy), Hotfile should have been held directly liable for copyright infringement of the distribution right.⁴³ Relying on both *Costar Group* and *Cablevision*, the court disagreed and concluded that the automatic conduct of software, unaided by human intervention, is not “volitional” and therefore Hotfile is not directly liable.⁴⁴

Although arguably expanded beyond its original purpose, not all courts are blindly applying *Netcom* immunity, as evidenced by the recent *Warner Brothers Entertainment, Inc. v. WTV Systems, Inc.* case, where the defendant unsuccessfully sought *Netcom* protection for its Zediva movie streaming service.⁴⁵ Using purchased copies of DVDs, defendant

³⁶ 633 F. Supp. 2d 124 (S.D.N.Y. 2009).

³⁷ *Id.* at 147-49.

³⁸ *Id.* at 130-31.

³⁹ *Id.* at 148.

⁴⁰ *Id.* at 148-49 (citing *Playboy Enters., Inc. v. Russ Hardenburgh, Inc.*, 982 F. Supp. 503, 503 (N.D. Ohio 1997)).

⁴¹ 798 F. Supp. 2d 1303 (S.D. Fla. 2011).

⁴² *Id.* at 1306.

⁴³ *Id.* at 1309.

⁴⁴ *Id.* at 1309-10 (citing *Costar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544, 550 (4th Cir. 2004) and *Cartoon Network, LLP v. CSC Holdings, Inc.*, 536 F.3d 121, 131 (2d Cir. 2008)).

⁴⁵ 824 F. Supp. 2d 1003, 1009 (C.D. Cal. 2011).

streamed or “transmitted” performances of the films via the Internet to its customers.⁴⁶ Because the customer initiated the viewing of the film by pressing a virtual button, defendants attempted to argue that it was the customer, not Zediva, that was performing the copyrighted works and therefore, that there was insufficient volition to find direct infringement of the public performance right by the service.⁴⁷ The district court rejected this argument and concluded that the fact that Zediva customers initiated the transmission by turning on their computers and choosing which film to view was immaterial — the service provider still transmitted a performance to the public.⁴⁸

A key factor in *WTV Systems* was that the party providing the Zediva service had discretion over what content was made available via streaming to its paying customers. In *Capitol Records, Inc. v. MP3tunes, LLC*, by contrast, the court addressed the volitional requirement in the context of the transmission of content claimed to have been uploaded or made available at the direction of users.⁴⁹ Plaintiff EMI alleged both direct and contributory infringement of the public performance right as a result of MP3tunes’ rebroadcast or transmission of songs.⁵⁰ MP3tunes is a music-focused “locker” service that also offered a related “Sideload” service. The Sideload service allowed users to “sideload” into their so-called lockers allegedly “free” music hosted on various third party sites, irrespective of whether said sites had authorization from the copyright owners to host the music.⁵¹ The Sideload Service also provided an index of these sites so that others could stream and “sideload” the same music to their own “lockers.”⁵² Apart from its search function, the Sideload service also generated lists of “Most Popular,” “Featured” and “New” songs that users could browse.⁵³ In addressing whether MP3tunes could be held directly liable under the transmit clause, the court concluded that, “MP3tunes’ on-line storage system utilizes automatic and passive software to play back

⁴⁶ *Id.* at 1007.

⁴⁷ *Id.* at 1009-10.

⁴⁸ *Id.* at 1010.

⁴⁹ 821 F. Supp. 2d 627, 649-50 (S.D.N.Y. 2011). MP3tunes is owned and operated by Michael Robertson, who is no stranger to copyright infringement claims, having been sued in 2000 for his MP3.com service. See *UMG Recordings, Inc. v. MP3.com, Inc.*, 92 F. Supp. 2d 349 (S.D.N.Y. 2000).

⁵⁰ *Capitol Records, Inc. v. MP3tunes, LLC*, 821 F. Supp. 2d at 649-50.

⁵¹ *Id.* at 647-48. In an attempt to justify its business model, MP3tunes argued that by offering a promotional download through an authorized Web site, EMI either abandoned its copyrights altogether or authorized downloads outside of the promotional context. *Id.*

⁵² *Id.* at 633-35.

⁵³ *Id.* at 634,

content stored at the direction of users . . . precisely the type of system routinely protected by the DMCA safe harbor.”⁵⁴

It therefore appears that despite the Second Circuit’s refusal in *Cablevision* to expand *Netcom* immunity to the public performance right, the *MP3tunes* court effectively did so. The court’s blatant sidestepping of whether MP3tunes was directly liable as a transmitter is indeed troubling from a copyright enforcement perspective, particularly since MP3tunes seemed to function more as a destination for music rather than a mere conduit or neutral service provider. From the consumer’s perspective, MP3tunes’ locker and “Sideload” services, together with the index of songs, appears to have functioned as a music streaming service just as the Zediva service functioned as a movie streaming service. And just as Webworld functioned as a destination for photos, MP3tunes appears to have functioned as a destination for music.

B. Under the Transmit Clause: Public or “Private” Performance?

In addition to facing potential expansion of *Netcom* immunity, copyright owners seeking to enforce their public performance right against Internet service providers face a separate issue — whether a transmission “to the public” (emphasis added) under the Copyright Act has taken place. As discussed below, the Second Circuit’s decision in *Cablevision* has created a technological loophole by which content providers may attempt to circumvent the transmit clause of the Copyright Act through the creation of unique — albeit temporary — copies from which each user’s transmission of a performance results.

Columbia Pictures Industries and *On Command Video* are the foundational cases that address what it means to publicly perform a work under the transmit clause of the Copyright Act, *i.e.*, to transmit or otherwise communicate a performance of a work to the public.⁵⁵ In *Columbia Pictures Industries v. Redd Horne*, the defendant operated stores offering video “showcasing” in small, private booths with a television.⁵⁶ Once the customer selected a film to watch, a store employee would insert that tape in one of the video cassette players (“VCP”) in the front of the store and transmit the film to the customer’s viewing booth.⁵⁷ The *On Command Video* case concerned a system for the electronic delivery of film videotapes to hotel guests.⁵⁸ The system consisted of a bank of VCPs centrally

⁵⁴ *Id.* at 650. See *infra* Section III.3.c(i)–(ii) for discussion of the court’s findings on Section 512 in *MP3tunes*.

⁵⁵ 17 U.S.C. § 101 (2006).

⁵⁶ 749 F.2d 154, 156–57 (3d Cir. 1984).

⁵⁷ *Id.* at 157.

⁵⁸ *On Command Video Corp. v. Columbia Pictures Indus.*, 777 F. Supp. 787, 789–90 (N.D. Cal. 1991).

located in the hotel's equipment room and connected to the hotel rooms.⁵⁹ When a hotel guests selected a particular movie to watch, the VCP containing that tape would transmit the film to that hotel room.⁶⁰ In both the *Columbia Pictures Industries* and *On Command* cases, there was only one videotape per film, and only one booth or room could receive the film at any one time. In an attempt to circumvent the public performance right, defendants in both cases unsuccessfully argued they were offering mere "electronic rentals" similar to the physical borrowing of videotapes.⁶¹ In both cases, the court found a violation of the public performance right, emphasizing that under the Copyright Act, a performance is still public "whether the members of the public . . . receive it in the same place or in separate places and at the same time or at different times."⁶² As stated by the *On Command* court, "the non-public nature of the place of the performance has no bearing on whether or not those who enjoy the performance constitute 'the public' under the transmit clause."⁶³

The Second Circuit in the *Cablevision* case, however, agreed with defendants' argument that the transmissions of recorded content to their paying RS-DVR subscribers were not "to the public" even though its RS-DVR service allowed subscribers to view the same programs at different times and places.⁶⁴ The programming was recorded at the direction of the subscriber, but was stored on and transmitted from Cablevision's RS-DVR servers. Cablevision's system stored a unique copy of each customer's recorded programming.⁶⁵ Ignoring the language of Section 106 of the Copyright Act which attaches the public performance right to the work and not a particular copy of the work, the Second Circuit reasoned that under the transmit clause, courts must examine the potential audience of a given

⁵⁹ *Id.* at 788.

⁶⁰ *Id.*

⁶¹ *Columbia Pictures Industries, Inc.*, 749 F.2d at 159-60; *On Command Video Corp.*, 777 F. Supp. at 789-90. The argument that the activity at issue constituted an "electronic rental" derived from the First Sale Doctrine, which prevents the copyright owner from controlling the future transfer of a particular copy once its material ownership has been transferred. Under the First Sale Doctrine, an establishment may rent or lease DVDs, books and/or video games without payment of a copyright royalty. See *Columbia Pictures Industries, Inc.*, 749 F.2d at 159-60. The *Columbia Pictures Industries* and *On Command Video* courts rejected this argument, holding that defendants' activities did not constitute a transfer of a copy but rather a public performance.

⁶² *Columbia Pictures Industries, Inc.*, 749 F.2d at 159; *On Command Video Corp.*, 777 F. Supp. at 790.

⁶³ *On Command Video Corp.*, 777 F. Supp. at 790.

⁶⁴ *Cartoon Network, LLP v. CSC Holdings, Inc.*, 536 F.3d 121, 137-40 (2d Cir. 2008).

⁶⁵ *Id.* at 137.

transmission to determine whether that transmission is “to the public.”⁶⁶ The court then held: “Because the RS-DVR system, as designed, only makes transmissions to one subscriber using a copy made by that subscriber, we believe that the universe of people capable of receiving an RS-DVR transmission is the single subscriber whose self-made copy is used to create that transmission.”⁶⁷ Therefore, no direct infringement of the public performance right was found in the *Cablevision* case. Aware of the potential technological loophole created by the decision, the Second Circuit cautioned that, “[t]his holding . . . does not permit content delivery networks to avoid all copyright liability by making copies of each item of content and associating one unique copy with each subscriber.”⁶⁸

Despite the Second Circuit’s cautionary language, there have been numerous attempts to expand application of the *Cablevision* private performance holding to new business models. For example, in *Warner Brothers Entertainment, Inc. v. WTV Systems, Inc.*, the defendants argued that under *Cablevision*, their “remote DVD playback transmissions,” as they called them, were not “to the public” because only one person was capable of receiving that transmission.⁶⁹ The defendants essentially sought to reduce each one-to-one Internet transmission to a private performance. The district court rejected the defendants’ arguments, and relying on *On Command* and *Redd Horne*, found direct infringement of the public performance right based on the fact that the defendants used the same DVD over and over again to transmit performances of the plaintiffs’ copyrighted works.⁷⁰ Given the absence of the existence and use of distinct copies, the court refused to expand *Cablevision*’s private performance ruling.⁷¹

In *Capitol Records, Inc. v. MP3tunes, LLC*, the master copy versus unique copy distinction from *Cablevision* resurfaced with regard to whether there was a public or private performance.⁷² Relying on *Cablevision*, plaintiffs argued on summary judgment that MP3tunes violated the public performance right because MP3tunes utilized a “master copy” to rebroadcast songs from the “lockers” to its customers (as opposed to storing a unique copy of content in each customer’s locker).⁷³ The district

⁶⁶ *Id.*

⁶⁷ *Id.*

⁶⁸ *Id.* at 139-40.

⁶⁹ 824 F. Supp. 2d 1003, 1011 n.7 (C.D. Cal. 2011).

⁷⁰ *Id.* Indeed, although developed approximately twenty years later, the Zediva system was analogous to the On Command system — instead of videotapes, the Zediva system used DVDs, instead of wired transmissions to hotel rooms, the Zediva system transmitted content from a central bank of DVD players to the consumer’s computer via an Internet connection.

⁷¹ *Id.*

⁷² 821 F. Supp. 2d 627, 649-50 (S.D.N.Y. 2011).

⁷³ *Id.*

court disagreed and took *Cablevision* one step further, concluding that the MP3tunes' system used a "standard data compression algorithm that eliminated redundant digital data," not a "master copy" system.⁷⁴ Tellingly, the court never explained why it mattered that a "standard data compression algorithm that eliminated redundant digital data" was used rather than a "master copy" system. Nonetheless, the court stated that reliance on *Cablevision* is "inapposite" because that case pertained to a cable provider, not an ISP. Ultimately, as mentioned, the court sidestepped the entire direct infringement analysis, concluding instead that MP3tunes' service should be subject to a Section 512 DMCA analysis, which is discussed below.⁷⁵

Most recently, through a strict application of *Cablevision*, the Southern District of New York denied plaintiffs, ABC, CBS, NBC and other copyright owners of over-the-air ("OTA") television programming a preliminary injunction against Aereo.⁷⁶ Through both its "Watch" and "Record" offerings, the Aereo service enables its customers to receive over-the-air (OTA) broadcast television via the Internet on their computers, smart phones or other enabled devices.⁷⁷ Plaintiffs sought a preliminary injunction only with regard to Aereo's "Watch" service, on the ground that this service essentially provides unauthorized retransmissions — in real time — of live OTA broadcast television programming, thus violating the transmit clause.⁷⁸ Under the Copyright Act, cable system operators and satellite carriers are required to pay a compulsory license to content owners for the retransmissions of broadcast programs, and Internet streaming has been held to fall outside of the Act's compulsory retrans-

⁷⁴ One could easily argue that the evidence adduced at the summary judgment stage indicated at minimum an issue of fact as to whether MP3tunes by virtue of its de-duplication of redundant data utilized a "master copy" to store and play back content. For example, the record revealed the following regarding the way MP3tunes' system functioned: If different users uploaded the same song containing identical blocks of data to MP3tunes' servers, those blocks will be assigned the same hash tag and typically will be saved only once. If a user plays a song from a locker, the storage system uses the hash tags associated with the uploaded song to reconstruct the exact file the user originally uploaded to his locker. *Id.* at 634.

⁷⁵ *Id.* See *infra* Section III.3.c(i)-(ii) for discussion of the court's findings on Section 512 in *MP3tunes*.

⁷⁶ *Am. Broad. Cos. v. Aereo, Inc.*, No. 12-1540, 2012 WL 2848158, at *1 (S.D.N.Y. July 11, 2012).

⁷⁷ *Id.* at *2.

⁷⁸ Memorandum of Points and Authorities in Support of Plaintiff's Joint Motion for a Preliminary Injunction at 7-9, *Am. Broad. Cos. v. Aereo, Inc.*, No. 12 Civ 1540 (S.D.N.Y. argued May 30, 2012).

mission licensing framework.⁷⁹ Aereo claimed under *Cablevision*, that any performance is private because all transmissions originate from a customer's unique copy made at their request.⁸⁰

As described by the district court, "[s]electing 'Watch' causes Aereo's system to transmit a web page to the user in which the program starts after a short delay, allowing the user to view the program 'live,' *i.e.*, roughly contemporaneous with its over-the-air broadcast."⁸¹ Upon selecting a broadcast program in "Watch" mode, the consumer's assigned antenna is activated and tuned into the station carrying the broadcast, a unique copy of the requested programming is made, and the transmission to the user results from that unique copy.⁸² In "Watch" mode, the user can also pause or rewind, which, as the court noted, increases the disparity between the time at which the program is initially broadcast and the time at which the user watches it.⁸³ The "Record" mode works similarly, with the main difference being that the copies made in "Record" mode are permanent — the copies made in the "Watch" function are not automatically retained.⁸⁴

Aereo argued that *Cablevision* insulated it from any liability for infringement of the public performance right. The plaintiffs attempted to distinguish the facts of *Cablevision* on the following grounds: Aereo's subscribers are watching the programs as they are still being broadcast, they are not using the copies Aereo creates for "time-shifting" as the customers were in *Cablevision*, and the Aereo copies do not "break[] the chain of the [over-the-air] transmission" received by Aereo.⁸⁵ The court rejected all of plaintiffs' efforts to distinguish *Cablevision*, noting three salient facts that place Aereo's "Watch" mode squarely within the *Cablevision* holding: (1) Aereo's system creates a unique copy of each television program for each subscriber who request to watch that program, saved to a unique directory on Aereo's hard disks assigned to that user; (2) each transmission that Aereo's system ultimately makes to a subscriber is from that unique copy; and (3) the transmission of the unique copy is made solely to the subscriber who requested it.⁸⁶ With regard to plaintiffs' argument that *Cablevision*'s holding was limited to situations of true time-shifting where

⁷⁹ 17 U.S.C. §§ 111(c) (cable systems), 111(a)(4), 119, 122 (satellite carriers); *see* WPIX, Inc. v. ivi, Inc., 765 F. Supp. 2d 594, 617 (S.D.N.Y. 2011) *aff'd*, 691 F.3d 275 (2d Cir. 2012) (2006).

⁸⁰ Aereo's Memorandum of Law in Opposition to Plaintiff's Motion for Preliminary Injunction on Copyright, at 2, *Am. Broad. Cos. v. Aereo, Inc.*, No. 12 Civ 1540 (S.D.N.Y. argued May 30, 2012).

⁸¹ *Aereo*, 2012 WL 2848158, at *2.

⁸² *Id.* at *3.

⁸³ *Id.* at *2.

⁸⁴ *Id.* at *4.

⁸⁵ *Id.* at *10.

⁸⁶ *Id.* at *11.

the initial broadcast of the programming was licensed, the district court stated, “time-shifting is simply not the basis of the Second Circuit’s [*Cablevision*] opinion” and “this Court remains obligated to apply the Circuit precedent with fidelity to its underlying reasoning.”⁸⁷ The concept of time-shifting stems from the Supreme Court’s decision in *Sony*, where the Court held that Sony was not contributorily liable for its distribution of the Betamax (VCR) television recorder because the device had a substantial non-infringing use, namely time-shifting of television programs, which the Court held was a fair use.⁸⁸ As mentioned, *Cablevision* did not involve claims of contributory liability—only claims for direct infringement.

An important issue in the case was the nature of the copies made by Aereo in “Watch” mode. Because a user’s unique copy of the programming was only retained until after the user finishes watching the program, plaintiffs argued that the copies were analogous to temporary buffer copies that are created when content is streamed.⁸⁹ Case law has confirmed that streaming constitutes a public performance under the transmit clause.⁹⁰

Given the way Aereo’s system was engineered, e.g., creating unique copies from a signal received by each user’s unique antenna, the court refused to find Aereo’s “Watch” copies to be purely facilitory.⁹¹ The court noted, “[t]here may be cases in which copies are purely facilitory, such as true buffer copies or copies that serve no function whatsoever other than to pass along a clearly identifiable ‘master’ copy from which the transmission is made.”⁹² Last, following *Cablevision*, the court refused to “look back (or ‘upstream’) to the point at which Aereo’s antennas obtain the broadcast content to conclude that Aereo engages in a public performance in retransmitting this content.”⁹³

C. *The Import of the Cases: Establishing Direct Infringement in the Context of File Hosting Services*

As the above discussion illuminates, copyright owners face many judicially-created obstacles in asserting claims for direct infringement in the context of file hosting services. First, the *Netcom* volitional standard

⁸⁷ *Id.* at *13.

⁸⁸ *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 437-38 (1984).

⁸⁹ *Aereo*, 2012 WL 2848158, at *17.

⁹⁰ *See, e.g.*, *United States v. ASCAP*, 627 F.3d 64, 74 (2d Cir. 2010); *WPIX, Inc. v. ivi, Inc.*, 765 F. Supp. 2d 594, 601 (S.D.N.Y. 2011); *Warner Bros. Entm’t, Inc.*, 824 F. Supp. 2d at 1011; *Video Pipeline, Inc. v. Buena Vista Home Entm’t, Inc.*, 192 F. Supp. 2d 321, 332 (D.N.J. 2002), *aff’d on other grounds*, 342 F.3d 191 (3d Cir. 2003).

⁹¹ *Aereo*, 2012 WL 2848158, at *21.

⁹² *Id.*

⁹³ *Id.* at *12.

evolved to protect passive conduits or neutral bulletin board services from direct liability. Over the years, we have seen *Netcom* expanded to services that are actively involved in serving up and serve as commercial destinations for a specific type of content. Given *Netcom* and its progeny, it will likely be difficult to establish direct liability against a file hosting service, such as Hotfile, where the content is uploaded at the direction of the user. We query whether the district court's decision in *Capitol Records v. MP3tunes* to simply skip over the direct liability analysis was correct given how involved MP3tunes was in indexing music on the Sideload service and the fact the MP3tunes functioned as a destination for music. Perhaps courts should revisit the approach of the *Webbworld* and *Arista v. UseNet* cases and deny *Netcom* immunity to a service that plays an active role in selecting the content to be offered or otherwise has involvement that transforms it from a passive provider to a commercial destination for content. Importantly, in the on-line world, a service's functions are almost always performed automatically as a result of software — this, in and of itself, should not defeat a finding of volition. We question whether the *Netcom* volitional standard, if not properly circumscribed to truly passive conduits and neutral file hosting services, will have been expanded too far in an effort to protect technology at the expense of copyright.

Second, technology shifts continue to challenge the scope of the public performance right, specifically the transmit right. While many of these technology shifts have increased efficiency, some of the new technologies were created solely in an attempt to circumvent the copyright laws by positioning themselves under the expanding umbrella of the *Cablevision* holding. The Copyright Act's definition of "to perform a work publicly" specifically includes a transmission right, i.e., "to transmit or otherwise communicate a performance or display of the work . . . by means of any device or process." Both the plain text and legislative history of the transmit clause indicate that it was meant to be broadly construed to cover not only the "initial rendition or showing" of a *work*, but also all further acts by which such "rendition or showing is transmitted or communicated to the public."⁹⁴ Congress made it clear in the legislative history that a performance or display may be accomplished by "any sort of transmitting ap-

⁹⁴ See H.R. REP. NO. 94-1476, at 63 (1976); see also 17 U.S.C. § 101 (2006) (defining publicly perform as including "to transmit . . . a performance . . . of the work . . . to the public, by means of any device or process, whether the members of the public capable of receiving the performance. . . receive it in the same place or separate places and at the same time or at different times") (emphasis added).

paratus, any type of electronic retrieval system, and any other techniques and systems not yet in use or even invented.”⁹⁵

Nonetheless, in the context of the public performance right, attempts to expand the *Cablevision* holding persist, as evidenced by the recent *Aereo* case. The technological distinction drawn by the district court between Aereo’s copies and buffer or facilitating copies provides little clarity or guidance and arguably widens *Cablevision*’s technological loophole. Although the court expressly rejected Aereo’s contention that “the creation of any fixed copy from which a transmission is made always defeats a claim for a violation of the public performance right”⁹⁶ — acknowledging that “[t]his position would eviscerate the transmit clause given the ease of making reproductions before transmitting digital data”⁹⁷ — the court’s rote application of *Cablevision* threatens to do just that. Upon appeal in the *Aereo* case, the Second Circuit may provide clarity and guidance in a way that honors the technological breadth and neutrality of the transmit clause and further does not blind itself to what the Aereo “Watch” function *actually does* — like a cable system operator, captures copyrighted OTA broadcasts and retransmits them to its own paying subscribers in virtual real time. If services can avoid liability merely by making a technological tweak or a temporary copy from which the transmission originates, what does this say about the way courts have construed the Copyright Act? The *Cablevision* court specifically stated that content delivery networks cannot avoid all copyright liability by enabling each subscriber to make their own individual copies.⁹⁸ Presumably, the Second Circuit’s cautionary language meant that *Cablevision*’s private performance ruling should be limited to its unique facts where the service is used for time-shifting and the original transmission of content was in fact authorized in the first place. In the world of so-called locker and cloud services that transmit content to users, a failure by courts to properly circumscribe the *Cablevision* ruling seriously threatens to upend the balance between copyright protection and innovation.

Obviously, it is impractical and inefficient to bring direct infringement actions against each of the vast number of individual infringing users. Given the potential difficulty in establishing direct liability against a file

⁹⁵ See H.R. REP. NO. 94-1476, at 64 (1976) (“The definition of ‘transmit’ . . . is broad enough to include all conceivable forms and combinations of wired or wireless communications media, including but by no means limited to radio and television broadcasting as we know them.”)

⁹⁶ *Am. Broad. Cos.*, Nos. 12 Civ 1540 (AJN), 12 Civ 1543, 2012 WL 2848158, at *21 (S.D.N.Y. July 11, 2012).

⁹⁷ *Id.*

⁹⁸ *Cartoon Network, LLP v. CSC Holdings, Inc.*, 536 F.3d 121, 139-40 (2d Cir. 2008).

hosting service, which allows users to upload the content, copyright owners often opt instead to assert claims of secondary infringement against the service itself. As shown below, judicial interpretation and application of the DMCA have also made it difficult for copyright owners to assert claims for secondary infringement against file hosting services.

III. SECONDARY LIABILITY AND THE DMCA

Given the potential difficulty in establishing sufficient volition for direct liability against a service, copyright owners increasingly rely on secondary liability to enforce rights against file hosting services that profit from their copyrighted content.⁹⁹ In recent cases brought against file hosting services, courts have construed the common law standards of contributory and vicarious liability in a relatively narrow manner and, as we explore below, have gone to great lengths to find DMCA safe harbor protection for the service providers. Below, we discuss the trend in these DMCA decisions away from imposing secondary liability on file hosting services or from imposing any obligation to cooperate with rights holders, other than through notice and takedown procedures. We conclude that courts generally have favored file hosting services over Bit Torrent and other peer-to-peer file sharing services, and, as a result, file hosting services that were built on encouraging and profiting from infringement have escaped liability under the DMCA. By contrast, in the peer-to-peer cases discussed below, i.e., *Grokster*, *Napster*, *Aimster*, *Columbia Pictures v. Fung*, *Arista v. Lime Group* and *Arista v. Usenet*, the DMCA defense was either rejected by the court or not asserted. We question whether there is a sound legal or policy basis underlying the favorable treatment of file hosting services.

For purposes of this article, we adopt the view that secondary liability encompasses two related, but distinct, theories — contributory liability and vicarious liability — and that inducement liability falls under the category of contributory liability. Although the Court in *Grokster* appeared to describe both inducement liability and *Sony* “staple-article-of-commerce” liability as forms of contributory infringement, noting there are “others,” a number of post-*Grokster* cases have treated inducement liability as a distinct form of secondary liability.¹⁰⁰ Under both contributory liability and

⁹⁹ See, e.g., *Arista Records v. Lime Group, LLC*, 715 F. Supp. 2d 481, 506 (S.D.N.Y. 2010). “The rationale for secondary liability is that a party who distributes infringement-enabling products or services may facilitate direct infringement on a massive scale, making it ‘impossible to enforce [copyright protection] effectively against all direct infringers.’” *Id.* at 506 (citing *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 929-30 (2005)).

¹⁰⁰ See 545 U.S. at 929-30; see also *Arista Records, LLC v. Lime Group, LLC*, 715 F. Supp. 2d at 481; *Arista Records, LLC v. Usenet.com, Inc.*, 633 F. Supp.

vicarious liability theories, a service provider potentially could be held liable for the direct infringement of a user. As a preliminary matter, under any theory of secondary liability, the direct infringement of another — e.g., the service provider's users — must first be established. The direct infringement of users is generally not difficult to establish with respect to any Internet service for which it can be shown that users are illegally uploading or downloading copyrighted content.¹⁰¹

A. Contributory Infringement

A contributory infringer has traditionally been defined as “one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another.”¹⁰² The Supreme Court in *Grokster* further defined contributory liability to include “intentionally inducing or encouraging direct infringement.”¹⁰³ The elements of a contributory infringement claim are: (i) actual *or* constructive knowledge of the infringement and (ii) material contribution to, or inducement of, the infringement. Courts have applied several different tests in the online environment to determine whether the provider of a service used by others for infringing purposes was contributorily liable.¹⁰⁴ The various standards for contributory liability are described below.

1. Material Contribution: Providing the Site and Facilities for Infringement

By the early 2000s, mass-scale online infringement through peer-to-peer file sharing technologies was firmly entrenched. One of the first contributory copyright infringement cases brought against an online service

2d 124, 150-549 (S.D.N.Y. 2009); *Columbia Pictures v. Fung*, No. 06-5578, 2009 WL 6355911 (C.D. Cal. Dec. 21, 2009) (distinguishing inducement liability from material contribution as separate forms of contributory liability); *but see* *Capitol Records, Inc. v. MP3tunes, LLC*, No. 07-9931, 2009 WL 3364036, at *4 (S.D.N.Y. Oct. 16, 2009) (dismissing plaintiffs' cause of action for inducement because it was not a separate claim from contributory liability).

¹⁰¹ See, e.g., *Arista Records, LLC v. Lime Group, LLC*, 715 F. Supp. 2d at 507.

¹⁰² *Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971).

¹⁰³ 545 U.S. at 934.

¹⁰⁴ For instance, the Court in *Grokster* described two main categories of contributory liability, the *Sony* standard of substantial non-infringing uses and the inducement standard under which it found the *Grokster* service liable, noting there are “others.” *Id.* at 929. See also *Capitol Records, Inc. v. MP3tunes, LLC*, 821 F. Supp. 2d 627, 646 (S.D.N.Y. 2011) (stating that, “[c]ontributory liability is premised on ‘personal conduct that encourages or assists the infringement’”) (quoting *Arista Records, LLC v. Doe 3*, 604 F.3d 110, 118 (2d Cir. 2010)).

provider that facilitated massive infringement was *A&M Records, Inc. v. Napster*.¹⁰⁵ The court in *Napster* found contributory liability based on the knowing provision of the site and facilities for infringement.¹⁰⁶ Napster had allowed its users to store MP3 music files on their own computers and to make the files available to other users.¹⁰⁷ Users were able to search for MP3 music files stored on other users' computers via the Napster peer-to-peer system.¹⁰⁸ Upon finding a file, users could then transfer an exact copy of the file from another's computer to the user's own computer and would make files on their own computers available for other users of the service.¹⁰⁹

The Ninth Circuit in *Napster* looked to the 1971 Second Circuit *Gershwin* case for the traditional standard of contributory liability: "one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another."¹¹⁰ The court held that Napster had "actual knowledge that specific infringing material [was] available using its system, that it could block access to the system by suppliers of the infringing material, and that it failed to remove the material."¹¹¹ The court also found that Napster materially contributed to the infringing activity because, without the services Napster provided, its users would not be able to find and download infringing music as easily from other users.¹¹² The court relied in particular on the brick and mortar case, *Fonovisa v. Cherry Hill*, in which the Ninth Circuit had found a swap meet operator contributorily liable for the infringement of vendors who sold pirate music cassettes from booths on the premises.¹¹³ There, the defendant was found to have knowledge of the infringement; it had been notified by the police that vendors were selling pirate music cassettes. The court also found that the swap meet operator provided the physical site, as well as other facilities (e.g., parking, restrooms, etc.), which permitted the infringing activity to take place. The Ninth Circuit in *Napster* extended this decision into the online world, finding that, because Napster knew of the infringement and provided the virtual "site and facilities" for the infringing conduct, Napster was contributorily liable for copyright infringement.¹¹⁴

¹⁰⁵ *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).

¹⁰⁶ *Id.* at 1020-22.

¹⁰⁷ *Id.* at 1011.

¹⁰⁸ *Id.*

¹⁰⁹ *Id.*

¹¹⁰ *Id.* at 1019 (citing *Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971)).

¹¹¹ *Id.* at 1022.

¹¹² *Id.* at 1022.

¹¹³ 76 F.3d 259, 264 (9th Cir. 1996).

¹¹⁴ See 239 F.3d at 1023; *Fonovisa*, 76 F.3d at 262.

By contrast, in *Perfect 10 v. RapidShare*,¹¹⁵ the court ruled that Perfect 10 was not likely to prevail on its claim of contributory infringement against cyberlocker service RapidShare — even though RapidShare had specific knowledge of its users' direct infringement.¹¹⁶ The court determined that RapidShare did not materially contribute to the infringement under the *Napster/Fonovisa* rule, it reasoned that the mere existence of a file hosting service was not sufficient for a finding of the provision of the site and facilities for infringement.¹¹⁷ The court distinguished RapidShare's service from the Napster service, stating that whereas Napster maintained a search engine of its directory of files, RapidShare did not index users' materials.¹¹⁸ Instead, an industry of third-party indexers assists users in finding illegal copies of copyrighted content on RapidShare hosted URLs.¹¹⁹

Napster was decided on far more general grounds, however. The court found that Napster provided the site and facilities for infringement because the service as a whole assisted users in locating and downloading infringing material. The fact Napster provided users with its own search tool was only one of several factors considered by the court, not the controlling factor. In focusing primarily on RapidShare's lack of a search tool, the court arguably lost sight of the overall purpose of the contributory liability standard — to hold responsible those who knowingly allow their

¹¹⁵ No. 09-CV-2596 H (S.D. Cal. May 18, 2010). RapidShare could not avail itself of the Section 512(c) safe harbor, because at the time the service did not have an agent designated with the U.S. Copyright Office for the receipt of takedown notices, a clear requirement under Section 512(c).

¹¹⁶ *Perfect 10, Inc. v. RapidShare, A.G.*, slip op. at 8-9.

¹¹⁷ *Id.*; but see *Capitol Records, Inc. v. MP3tunes, LLC*, 821 F. Supp. 2d 627, 648-49 (S.D.N.Y. 2011) (finding contributory liability for the copies of infringing materials in users' lockers on the MP3tunes locker service—which the service had failed to remove after receiving notice of the original uploaded copy—on the grounds that its service substantially contributed to the infringing activity by providing the “site and facility” for the infringing activity and MP3tunes’ “knowledge of infringing sideloaded material [was] manifest.”).

¹¹⁸ *Perfect 10, Inc. v. RapidShare, A.G.*, slip op. at 8-9. The court also found that the plaintiff had not met its burden of showing that RapidShare was liable for inducing infringement under the *Grokster* inducement rule (confusing it with the *Sony* discussion of the *Grokster* rule) because RapidShare's service has “substantial lawful uses” and it “strives to eliminate infringing uses.” See *id.* at 11.

¹¹⁹ When a user posts a file to RapidShare, the user is given a URL. The default at the time of suit was that the URL would be publicly accessible, so anyone having the URL address could access the file located at the URL. Indexing services arose which allowed the public to search for specific content on the RapidShare service not specifically designated as private.

services to be used for infringement and who could, but fail to, take simple measures to stop the infringement.¹²⁰

2. *Material Contribution: Ability to Prevent Further Damage but Failure to Do So*

The Ninth Circuit in *Perfect 10 v. Amazon.com* sought to derive a single standard from the common law precedent for contributory infringement in an electronic environment — what it called a “refined” test “in the context of cyberspace.”¹²¹ It adopted a test for contributory infringement that it ascribed to *Napster* and *Netcom*,¹²² where the operator has “actual knowledge that specific infringing material is available using its system” and can “take simple measures to prevent further damage” to copyrighted works, yet continues to provide access.¹²³ The court explained that both *Napster* and *Netcom* “ruled that a service provider’s knowing failure to prevent infringing actions could be a basis for imposing

¹²⁰ Since the time of this suit and lawsuits filed against it in Germany, RapidShare has adopted new policies to reduce infringing uses and has announced a proactive policy to counter infringing activity on its service. It states that it now scans incoming files to make sure the files do not have the same signature as files previously blocked; no longer compensates users for high download volumes (and recommends that it be verified that the user is a rightful owner before any such compensation is provided), recommends that the default be private and not public URLs, and employs staff to police the site. An RIAA spokesperson welcomed RapidShare’s efforts and recognition of its “shared responsibility to prevent theft,” but said the measures fall short since RapidShare’s business model is still to allow “unlimited distribution of copyrighted files among millions of anonymous strangers” as compared to storage lockers that provide secure storage for users’ files. Timothy B. Lee, *RapidShare Struggles to Placate Big Content with Anti-Piracy Plan*, ARSTECHNICA (Apr. 19, 2012, 2:45 PM), <http://arstechnica.com/tech-policy/2012/04/rapidshare-struggles-to-placate-hollywood-with-anti-piracy-plan>.

¹²¹ 508 F.3d 1146, 1171 (9th Cir. 2007).

¹²² In *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361, 1365-66 (N.D. Cal. 1995), the court had found that neither the bulletin board operator nor the Internet access provider, Netcom, was contributorily liable for the infringing posts of a user. The plaintiffs, owners of copyrights in the works of Scientology founder L. Ron Hubbard, asserted that Netcom was liable as a contributory infringer because it, “with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another.” *Id.* at 1373 (quoting *Gershwin Publ’g Corp. v. Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971)). The court viewed the “with knowledge” standard through a timeliness lens, finding that Netcom did not “knowingly” contribute to the infringement because it did not have knowledge in time to do anything about the infringement. *Id.* at 1374.

¹²³ *Perfect 10, Inc. v. Amazon.com*, 508 F.3d at 1171.

contributory liability.”¹²⁴ This focus on the defendant’s ability to mitigate damage is also reflected in the *Aimster* case, described below, in which Judge Posner placed the burden on the service provider if the infringement is substantial and it is in the better position to mitigate the infringement.¹²⁵ Under this standard, the court in *Perfect 10 v. Google* found that Google had substantially assisted (i) Web sites in distributing infringing content worldwide and (ii) users in accessing infringing content worldwide, but the court remanded on the issues of whether Google had reasonable and feasible means to refrain from providing access and whether it had knowledge by virtue of Perfect 10’s notices.¹²⁶

3. Sony Test: Supplying a Product that is Used to Infringe

Under the Supreme Court’s ruling in *Sony v. Universal City Studios*¹²⁷ a defendant may be found contributorily liable if it supplies a product with the intent that customers use the product to make unauthorized copies of copyrighted material. The Court in *Sony* stated that such an intent to induce infringement can be deduced if, and only if, the product supplied is a “staple article of commerce” that is not suitable for substantial non-infringing uses.¹²⁸ The producer of a product that does have substantial non-infringing uses is not a contributory infringer merely because some of the uses actually made of the product are infringing. The Court held that Sony was not contributorily liable for its distribution of the Betamax (VCR) television recorder at issue in the case because the device had a substantial non-infringing use, namely time-shifting of television programs, which the Court held was a fair use.¹²⁹

4. Willful Blindness as Knowledge

The Seventh Circuit in the *Aimster* case found knowledge sufficient for contributory infringement, but did so based on a theory of “willful blindness,” as opposed to actual knowledge.¹³⁰ *Aimster* was a peer-to-peer service developed in the wake of *Napster*. In an effort to shield them-

¹²⁴ *Id.* at 1172 (citing *A&M Records, Inc. v. Napster*, 239 F.3d 1004, 1022 (9th Cir. 2001) and *Netcom*, 907 F. Supp. at 1375).

¹²⁵ *In re Aimster Copyright Litigation*, 334 F.3d 643, 653 (7th Cir. 2003). (“Even when there are infringing uses of an Internet file-sharing service, moreover, if the infringing uses are substantial then to avoid liability as a contributory infringer the provider of the service must show that it would have been disproportionately costly for him to eliminate or at least reduce substantially the infringing uses.”).

¹²⁶ 508 F.3d at 1172-73.

¹²⁷ 464 U.S. 417 (1984).

¹²⁸ *Id.* at 442.

¹²⁹ *Id.*

¹³⁰ *Aimster*, 334 F.3d at 650.

selves from liability, the defendants who operated the service implemented encryption software that prevented them from knowing what specifically was being shared through the service. As such, the defendants argued, they did not have the requisite knowledge of the infringement occurring on their file-sharing service.¹³¹ The court readily found material contribution to the infringement, as had the court in *Napster*, on the grounds that the defendants' service facilitated infringement and did nothing to stop it. Then, likening the defendants' behavior to a drug trafficker who "[s]eeks to insulate himself from the actual drug transaction so that he c[an] deny knowledge of it,"¹³² the court also found that the defendants' attempt to shield themselves from knowing of any specific infringement amounted to willful blindness.

The Seventh Circuit equated the defendants' willful blindness with constructive knowledge, sufficient to find that the defendants had knowingly and materially contributed to the infringement.¹³³ It held that Aimster's willful blindness could not shield it from liability and that the copyright law, like the criminal law, does not differentiate between willful blindness and actual knowledge in judging a defendant's culpability.¹³⁴ The court also denied the defendants protection under the Supreme Court's *Sony* decision, noting that they had failed to demonstrate that the Aimster service *actually had* substantial non-infringing uses, as opposed to *being merely capable* of non-infringing uses.¹³⁵ In view of the Aimster defendants' willful blindness and the fact that their service was used exclusively for infringement of the plaintiffs' copyrighted music, the court also rejected application of the DMCA safe harbor defense.¹³⁶

5. Grokster Test: Actively Encouraging or Inducing Infringement

The Supreme Court in *Grokster* distinguished "inducement" liability from the "staple-article-of-commerce" form of contributory infringement

¹³¹ *Id.*

¹³² *Id.*

¹³³ *Id.*

¹³⁴ *Id.* In the recent Second Circuit decision, *Viacom International v. YouTube*, the court discussed willful blindness in the context of the Section 512(c) defense, and held that "the willful blindness doctrine may be applied, in appropriate circumstances, to demonstrate knowledge or awareness of specific instances of infringement under the DMCA," but that willful blindness in the DMCA context could never require any affirmative duty to monitor. The court remanded to the district court the question of "whether the defendants made a 'deliberate effort to avoid guilty knowledge.'" 676 F.3d 19, 35, 41-42 (2d Cir. 2012) (citing *Aimster*, 334 F.3d at 650).

¹³⁵ *Aimster*, 334 F.3d at 655 (citing *Sony*, 464 U.S. 417).

¹³⁶ *Id.* at 655.

at issue in the *Sony* decision.¹³⁷ The Court explained that the “staple article-of-commerce” test applied in *Sony* is applicable only where there is no direct evidence of culpable intent to promote infringement.¹³⁸ In such cases, intent to encourage infringement could be inferred from the nature of the product itself, but only if it had no substantial non-infringing use.¹³⁹

In *Grokster*, by contrast, the Court found that there was direct evidence of unlawful intent to actively induce infringement. The Court applied the basic standard for contributory infringement — whether the defendants had in fact “intentionally induc[ed] or encourage[ed] direct infringement” — and noted that a court may find an intent to induce infringement where evidence “shows statements or actions directed to promoting infringement.”¹⁴⁰ As the *Grokster* court stated, “where evidence goes beyond a product’s characteristics or the knowledge that it may be put to infringing uses, and shows statements or actions directed to promoting infringement, *Sony*’s staple-article rule will not preclude liability.”¹⁴¹

In *Grokster*, the defendants had “distribute[d] free software products that allow[ed] computer users to share electronic files through peer-to-peer networks.”¹⁴² The Court found liability based on evidence establishing that the defendants had the unlawful purpose of promoting copyright infringement, including evidence in the record that the defendants engaged in intentional attempts to attract former Napster users.¹⁴³ Internal documents and tactics showed a clear intent and design to attract such users, coupled with the defendants’ failure to implement filtering tools to diminish the infringing activity.¹⁴⁴ In addition, the defendants profited from increased traffic since they made money by selling advertising space.¹⁴⁵ The Court explained that, since “the extent of the software’s use determines the gain to the distributors, the commercial sense of their enterprise turns on high-volume use, which the record shows is infringing-

¹³⁷ *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 930 (2005) (citing *Sony*, 464 U.S. 417 (1984)).

¹³⁸ *Id.* at 931-32 (discussing *Sony*, 464 U.S. at 439, 442).

¹³⁹ *Id.* at 932-34. The Court stated that the *Sony* theory of liability is based on imputing culpable intent as a matter of law from the characteristics of the distributed product where there is no direct evidence of intent, but that *Sony* did not foreclose fault based contributory liability (such as existed in *Grokster*).

¹⁴⁰ *Id.* at 934-35.

¹⁴¹ *Id.* at 933.

¹⁴² *Id.* at 918.

¹⁴³ *Id.* at 938.

¹⁴⁴ *Id.* at 939.

¹⁴⁵ *Id.*

ing.”¹⁴⁶ The Court concluded that there was sufficient evidence to support a finding that the defendants intended to promote their service to infringe copyright.¹⁴⁷

Several more recent peer-to-peer file sharing cases have similarly found inducement infringement on summary judgment.¹⁴⁸ In *Arista v. Lime Group*, *Arista v. Usenet* and *Columbia Pictures v. Fung*, district courts analyzed inducement infringement separately from contributory infringement and found defendants secondarily liable for inducement infringement.¹⁴⁹

In *Arista Records, LLC v. Lime Group, LLC*,¹⁵⁰ the court held that the defendants, owners of the file sharing service LimeWire, were liable for contributory infringement where (1) the defendants engaged in purposeful conduct that encouraged infringement and did so (2) with the intent to encourage such infringement. The court looked to a number of factors to establish that the defendant intended to encourage infringement, namely, the defendant’s: (1) awareness of substantial infringement by users, (2) efforts to attract infringing users, (3) efforts to enable and assist users to commit infringement, (4) dependence on infringing use for the success of its business, and (5) failure to mitigate infringing activities.¹⁵¹ After analyzing each of these factors in light of the evidence, the court concluded that the defendant had intended to encourage infringement and was therefore liable.¹⁵² The *Arista v. Lime Group* decision includes no discussion of the DMCA safe harbor defense.

In *Arista v. Usenet.com*, the plaintiff recording companies challenged operators of a file distribution service, which allegedly made copyright music available for users to download.¹⁵³ Among other claims, the plain-

¹⁴⁶ *Id.* at 940.

¹⁴⁷ *Id.* at 936-37.

¹⁴⁸ Many current file sharing services use more sophisticated forms of peer-to-peer technologies than used by the *Napster* and *Grokster* defendants. BitTorrent, for instance, is a commonly used file sharing system that enables users to distribute large amounts of data over the Internet. The system allows users to join a number of hosts to download and upload from one another at the same time. Files are divided into several pieces and distributed out to users. When a piece is received by a user that user now becomes a source for others to download from.

¹⁴⁹ *Arista Records, LLC v. Lime Group, LLC*, 715 F. Supp. 2d 481 (S.D.N.Y. 2010); *Arista Records v. Usenet*, 633 F. Supp. 2d at 150-54; *Columbia Pictures v. Fung*, No. 06-5578, 2009 WL 6355911 (C.D. Cal. Dec. 21, 2009). All three of these cases involved file sharing services that employed variations of peer-to-peer technology.

¹⁵⁰ 715 F. Supp. 2d at 481.

¹⁵¹ *Id.* at 508.

¹⁵² *Id.* at 515.

¹⁵³ 633 F. Supp. 2d 124, 124 (S.D.N.Y. 2009).

tiffs alleged inducement of copyright infringement. The court compared the facts with *Grokster* and found the cases to be similar, noting that the service was used primarily to obtain copyrighted material and the widespread availability of infringing content on the service was obvious.¹⁵⁴ In addition, internal documents and other evidence indicated that the defendants sought to attract Napster and Kazaa users, including by use of meta tags in source code to attract searches for these infringing services to defendants' own service. There was also evidence that employees had downloaded infringing material from the service. Furthermore, evidence established that defendants did not implement blocking or filtering technology that was available to it.¹⁵⁵ Based on this and other evidence, the court granted plaintiffs' motion for summary judgment for inducement of infringement. Given the defendants' spoliation of evidence, the court precluded assertion of the DMCA defense, noting also that if defendants "encouraged or fostered such infringement, they would be ineligible for the DMCA's safe harbor provisions."¹⁵⁶

In *Columbia Pictures v. Fung*, plaintiffs, major motion picture studios, sued Fung for the set-up, maintenance, and operation of a BitTorrent type of peer-to-peer file sharing service.¹⁵⁷ The plaintiffs claimed that the service, by design, fostered wide-scale copyright infringement by users.¹⁵⁸ Fung's service, IsoHunt, provides users with the access to other users' computers to allow users to download various content, including plaintiffs' movies and television programs. The court analyzed whether Fung was secondarily liable for inducement infringement and looked to *Grokster* for the rule that "inducement requires that the defendant has undertaken purposeful acts aimed at assisting and encouraging others to infringe copyright."¹⁵⁹ It found that the evidence for Fung's inducement of copyright infringement was "overwhelming and beyond reasonable dispute."¹⁶⁰ Fung disseminated messages to users encouraging them to commit infringement, assisted users in committing infringement and implemented technical features probative of the intent to induce infringement.¹⁶¹ Additionally, Fung's business model depended on continuous infringing use further supporting the claim for contributory liability.¹⁶² The court rejected any application of the DMCA safe harbor defense on the grounds

¹⁵⁴ *Id.* at 152-55.

¹⁵⁵ *Id.*

¹⁵⁶ *Id.* at 142.

¹⁵⁷ No. 06-5578, 2009 WL 6355911, at *2-3 (C.D. Cal. Dec. 21, 2009).

¹⁵⁸ *Id.*

¹⁵⁹ *Id.* at *7 (citing *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 936-37 (2005)).

¹⁶⁰ *Id.* at *11.

¹⁶¹ *Id.* at *11-13.

¹⁶² *Id.* at *14.

that it was incompatible with defendants' "'purposeful, culpable expression and conduct' aimed at promoting infringing uses of the Web sites."¹⁶³

As seen in the above cases, courts have not hesitated to impute an intent to induce direct infringement in the peer-to-peer cases where a combination of factors has collectively demonstrated such an intent. These factors include: providing systems, technologies or advice that assist the users in finding the infringing content, actively attempting to attract infringers, knowledge that infringement on its site is abundant, the business' dependency on the infringement for growth, and the service provider's ability to take simple measures to prevent further damage to copyrighted works, but failure to do so.¹⁶⁴

Many of the same factors are present with respect to file hosting services that cater to infringement. Copyright owners have not fared as well, however, on claims of contributory liability, including inducement liability, even where the evidence suggest that the same factors described above are present, such as where the service allows or even encourages the uploading of infringing content. This is due in large part to the fact that in most of the recent cases brought against file hosting services, the courts found that the Section 512(c) safe harbor applied. The services in these cases had a registered agent for receiving DMCA notices and were able to show that they complied with specific DMCA takedown notices that precisely specified the infringing item and its location.¹⁶⁵ But, it may also relate to the fact that these services generally have some legitimate uses, as suggested by the *dicta* in many of the cases. Even though, as the Court in *Grokster* explained, the existence of substantial non-infringing uses does not negate a finding of inducement, it does lend these services some legitimacy and appears to have influenced the outcome of some of the cases.¹⁶⁶

For instance, in *Viacom International v. YouTube*, during the 2005–2006 period at issue,¹⁶⁷ when between 70–80% of the content on the site was infringing by YouTube's own estimates, arguably, most, if not all, of the factors for inducement infringement were present: YouTube provided a system, technologies and advice (e.g., links to recommended similar videos) that assisted users in finding the infringing content; the e-mail

¹⁶³ *Id.* at *18 (quoting *Grokster*, 545 U.S. at 937).

¹⁶⁴ See *Arista Records, LLC v. Lime Group, LLC*, 2010 U.S. Dist. LEXIS 46638, at *56–57, 73 (S.D.N.Y. May 11, 2010); *Arista Records, LLC v. Usenet.com, Inc.*, 633 F. Supp. 2d 124, 151–52 (S.D.N.Y. 2009).

¹⁶⁵ See *infra* Section III.3.c.

¹⁶⁶ 545 U.S. at 929.

¹⁶⁷ 718 F. Supp. 2d 514, 529 (S.D.N.Y. 2010), *rev'd and remanded in part and aff'd in part*, 676 F.3d 19 (2d Cir. 2012). A separate class action case brought by several associations and music publishers against YouTube, *The Football Association Premier League, Limited*, was joined to the case and alleged continuing current infringement.

record showed that YouTube knew that infringement on its site was abundant; the founders believed and reminded each other that the business was dependent on the infringement for growth; and YouTube had the ability to take simple measures to prevent further damage to copyrighted works (it had a filtering system that it refused to use for Viacom and had taken other anti-infringement measures but quickly discontinued them).¹⁶⁸ Yet, the district court in *Viacom v. YouTube* stated:

The *Grokster* model does not comport with that of a service provider who furnishes a platform on which its users post and access all sorts of material as they wish, while the provider is unaware of its content, but identifies an agent to receive complaints of infringement, and removes identified material when he learns it infringes.¹⁶⁹

It should be noted that the district courts in both *UMG Recordings v. Veoh Networks* and *Viacom, Inc. v. YouTube, Inc.* never actually addressed the issue of inducement infringement because they addressed the issue of safe harbor eligibility first, prior to analyzing whether the defendant was secondarily liable in the first instance.¹⁷⁰ If the service provider is covered by Section 512, then, courts assume they do not need to reach the issue of underlying liability, even when inducement liability has been pled. The district court in *Viacom, Inc. v. YouTube, Inc.*, for instance, dismissed on summary judgment Viacom's claims for direct, vicarious and contributory infringement (including inducement) without comment because it found YouTube qualified under Section 512(c).¹⁷¹ The Second Circuit upheld the district court's determination "that a finding of safe harbor application necessarily protects a defendant from all affirmative claims for monetary relief."¹⁷²

¹⁶⁸ Memorandum of Law in Support of Viacom's Motion for Partial Summary Judgment on Liability and Inapplicability of the Digital Millennium Copyright Act Safe Harbor Defense at 10, *Viacom Int'l, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514 (S.D.N.Y. 2010), *aff'd in part, vacated in part*, 676 F.3d 19 (2d. Cir. 2012).

¹⁶⁹ 718 F. Supp. 2d at 526. The implication of the district court's conclusion is that a service that complies with DMCA notice and takedown ipso facto cannot be found guilty of inducing infringement. The interaction between inducement liability and Section 512 eligibility, discussed below, is an interesting one that has not been fully explored in the case law. See *infra* Section III.3.c(i).

¹⁷⁰ See, e.g., 620 F. Supp. 2d 1081 (C.D. Cal. 2008), *aff'd*, *UMG Recordings, Inc. v. Shelter Capital Partners*, 667 F.3d 1022, 1031-35 (9th Cir. 2011)); 718 F. Supp. 2d at 526; *Io Group, Inc. v. Veoh Networks*, 586 F. Supp. 2d 1132, 1146 (N.D. Cal. 2008); *Perfect 10, Inc. v. CCBill, LLC*, 488 F.3d 1102, 1112 (9th Cir. 2007).

¹⁷¹ 718 F. Supp. 2d at 529.

¹⁷² *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d at 41.

Section 512 only protects against monetary liability, however, and does provide for limited injunctive or equitable relief under Section 512(j) (although to date this relief has never been granted).¹⁷³ The courts' unwillingness to consider liability if Section 512 protection is granted means that this injunctive relief is automatically denied the plaintiff. Moreover, by addressing Section 512 eligibility in a vacuum and applying such different standards for the Section 512 eligibility criteria than the secondary liability standards Congress based them on, the courts have allowed themselves to avoid difficult issues of culpability.¹⁷⁴ Arguably, if a court is forced to look at liability in the first instance, particularly inducement liability, it might be less inclined to interpret the Section 512 "knowledge" and "control" standards so differently from the analogous and longstanding common law standards for contributory and vicarious liability. One might see more decisions like *Aimster* and *Fung*, where, the defendant's "bad faith conduct to promote infringement," i.e., its culpability, is so clear after viewing the conduct through the lens of secondary liability that the court would find it absurd to then turn around and provide the defendant with DMCA safe harbor protection.¹⁷⁵

B. Vicarious Liability

An entirely separate basis for secondary liability is the doctrine of vicarious liability, which stems from the common law of torts. A defendant is vicariously liable for the actions of a direct infringer where the defendant (i) has the right and ability to control the infringer's acts *and* (ii) receives a direct financial benefit from the infringement.¹⁷⁶ Unlike contributory liability, lack of knowledge that the primary infringer has engaged in infringing conduct is not a defense. For instance, courts have found the owner of a place of entertainment liable for infringements occurring on the premises, where the owner actively operated or supervised

¹⁷³ See *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090 (W.D. Wash. 2004); *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132 (N.D. Cal. 2008); *Perfect 10 v. Google*, 508 F.3d at 1175; *Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229 (D.C. Cir. 2003); *In re Subpoena to Univ. of North Carolina at Chapel Hill*, 367 F. Supp. 2d 945 (M.D.N.C. 2005); *A & M Records, Inc. v. Napster, Inc.*, 54 U.S.P.Q.2d 1746 (N.D. Cal. 2000).

¹⁷⁴ See *infra* Section III.3.c.

¹⁷⁵ See *In re Aimster Copyright Litigation*, 334 F.3d 643, 655 (7th Cir. 2003); *Columbia Pictures v. Fung*, No. 06-5578, 2009 WL 6355911, at *18 (C.D. Cal. Dec. 21, 2009). See also *Arista Records, LLC v. Usenet.com, Inc.*, 633 F. Supp. 2d 124, 142 (S.D.N.Y. 2009).

¹⁷⁶ *Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc.*, 907 F. Supp. 1361, 1375 (N.D. Cal. 1995).

the operation of the establishment, even though the infringing acts occurred without the owner's authority or against his orders.¹⁷⁷

In *Napster* and other peer-to-peer cases, the courts found that the first element of vicarious liability, the right and ability to control, was met where it could be established that the file hosting service had the right and ability to control the infringing uses by blocking infringers' access to the service or by removing infringing content.¹⁷⁸ As the court in *Napster* stated: "[t]he ability to block infringers' access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise."¹⁷⁹ In *Napster*, the defendant had an express reservation of rights policy stating that it expressly reserved the "right to refuse service and terminate accounts in its discretion, including, but not limited to, if Napster believes that user conduct violates applicable law . . . or for any reason in Napster's sole discretion, with or without cause."¹⁸⁰ This was deemed sufficient to establish that Napster retained the right to control access to its system.

In *Perfect 10 v. Google*, by contrast, the Ninth Circuit found that Google did not have the right and ability to control the infringing Web sites because it has no contractual rights or parity with those sites. The court distinguished Google image search from Napster because the Napster system was closed and it had the right to terminate users' accounts and block access to its system; whereas, Google could not stop the infringing activity because that activity occurs on third-party Web sites over which it has no control.¹⁸¹ Under the Ninth Circuit's reasoning in *Perfect 10 v. Google*, file hosting services would be in the same position as Napster, not Google, in that the services require registration and agreement to terms of use, generally which enable the file host to terminate users, and the file host has the actual ability to remove or block infringing material.¹⁸²

¹⁷⁷ *Famous Music Corp. v. Bay State Harness Horse Racing & Breeding Ass'n*, 554 F.2d 1213, 1214-15 (1st Cir. 1977); *see also* *Range Road Music, et al. v. East Coast Foods*, 668 F.3d 1148 (9th Cir. 2012).

¹⁷⁸ *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1023-24 (9th Cir. 2001). *See* *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 930-31 (2005); *Aimster*, 334 F.3d at 654-55; *Perfect 10, Inc., v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1173-74 (C.D. Cal. 2002).

¹⁷⁹ 239 F.3d at 1023.

¹⁸⁰ *Id.*

¹⁸¹ *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1173-74 (9th Cir. 2007) ("Google cannot terminate those third-party web sites or block their ability to host and serve infringing full-size images . . .").

¹⁸² *See, e.g., Arista Records, LLC v. Lime Group, LLC*, 715 F. Supp. 2d 481, 518 (S.D.N.Y. 2010); *Arista Records, LLC v. Usenet.com, Inc.*, 633 F. Supp. 2d 124, 157 (S.D.N.Y. 2009).

With respect to the second element of vicarious liability, financial benefit from the infringement, courts have generally agreed that “[f]inancial benefit exists where the availability of infringing material ‘acts as a draw’ for customers.”¹⁸³ For instance, in a bricks and mortar vicarious liability case, *Famous Music*, the race track owner was vicariously liable for the company who supplied the music that entertained the patrons at the track, as the owner was profiting from of the infringing music.¹⁸⁴ Similarly, in *Fonovisa, Inc. v. Cherry Auction, Inc.*, the court held that “the sale of pirated recordings at the Cherry Auction swap meet [was] a ‘draw’ for customers, as was the performance of pirated music in dance hall cases and their progeny.”¹⁸⁵

In the on-line world, courts have applied the “financial benefit from the infringement” requirement with mixed results. In the pre-DMCA *Netcom* case, in determining that Netcom did not receive a direct benefit from the infringement, the court relied on the fact that Netcom received a fixed fee from all users, with no relation to whether they were engaged in infringing activities.¹⁸⁶ In *Ellison v. Robertson*, the court held that AOL did not receive a direct financial benefit from providing access to infringing content, finding no evidence that AOL gained subscriptions because of the infringement.¹⁸⁷ The court in *Napster*, on the other hand, held that Napster received a “direct financial benefit” because Napster’s future advertising revenue was directly dependent upon increases in user base and the infringing material was a draw for users.¹⁸⁸ Similarly, in both *Arista Records, LLC v. Usenet.com*¹⁸⁹ and *Arista Records, LLC v. Lime Group, LLC*,¹⁹⁰ the Southern District of New York held that the infringing content was a draw for users, sufficient to show a direct causal nexus between the infringement and the financial benefit to the defendant. In *Arista Records v. Usenet*, the court noted that the draw need not be the primary, or even a significant, draw — rather, it need only be “a draw.”¹⁹¹

¹⁸³ *Napster*, 239 F.3d at 1023.

¹⁸⁴ *Famous Music Corp. v. Bay State Harness Horse Racing & Breeding Ass’n*, 554 F.2d 1213, 1214-15 (1st Cir. 1977).

¹⁸⁵ 76 F.3d 259, 263-64 (9th Cir. 1996). The dance hall cases held the halls liable where infringing “activities provide the [dance halls] with a source of customers and enhanced income.” See also *Range Road Music, Inc.*, 668 F.3d 1148 (9th Cir. 2012).

¹⁸⁶ *Religious Tech. Ctr. v. Netcom On-Line Commc’n Servs., Inc.*, 907 F. Supp. 1361, 1377 (N.D. Cal. 1995).

¹⁸⁷ 357 F.3d 1072, 1079 (9th Cir. 2004).

¹⁸⁸ 239 F.3d at 1023.

¹⁸⁹ 633 F. Supp. 2d 124, 157 (S.D.N.Y. 2009).

¹⁹⁰ 715 F. Supp. 2d 481, 518 (S.D.N.Y. 2010).

¹⁹¹ 633 F. Supp. 2d at 157.

In the case of Internet file hosting services, right and ability to control should be established, as most of these types of services require user registration and agreement to terms of use and maintain the ability to terminate users and remove content. For file hosting services, a financial benefit should be found where the infringing content simply draws more users to the site and thereby increases the service's overall value, allowing the owners of the service to profit from a sale of all or part of the service (and in some cases, thereby acquiring a personal fortune).¹⁹² Thus, if the availability of infringing content is a draw for users, which in turn increases revenue or value, then the "financial benefit" factor should be deemed to have been met. For instance, as alleged in the *Disney v. Hotfile* case, if most consumers who pay for "premium" services, which offer increased storage capacity, faster service and longer periods of storage, use the service for infringing purposes, then it should be possible to demonstrate the necessary causal connection between the financial benefit and the infringement.¹⁹³

As discussed, however, the trend in these file hosting cases is for courts to first analyze whether the provider meets the requirements under the Section 512 safe harbor, and if the court finds the provider does, no separate vicarious liability analysis will be conducted. As such, there is scant case law on vicarious liability in the first instance in copyright infringement cases against file hosting services. Although the vicarious liability standard is imported word-for-word into Section 512, courts have imposed a heightened standard in the Section 512 context, as discussed below, and as a result, have created a heightened standards for establishing vicarious liability of a file hosting service.¹⁹⁴

C. Section 512(c) Safe Harbor Protection

The Section 512 safe harbor requirements were intended to provide strong incentives for service providers to cooperate with rights holders by offering innocent service providers protection for liability for user in-

¹⁹² YouTube, for instance, was sold to Google in a stock-for-stock transaction valued at \$1.65 billion dollars, with two of the founders personally profiting over \$ 300 million from the sale. See *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 28 (2d Cir. 2012); *Google Buys YouTube for \$1.65 Billion*, MSNBC.COM (Oct. 10 2006), http://www.msnbc.msn.com/id/15196982/ns/business-us_business/t/google-buys-youtube-billion/#.T5lgPRxq7Ek ("Internet search leader Google is snapping up YouTube for \$1.65 billion, brushing aside copyright concerns to seize a starring role in the online video revolution.").

¹⁹³ 798 F. Supp. 2d 1303, 1306-07 (S.D. Fla. 2011).

¹⁹⁴ See *infra*, at Section III.3.c(ii).

fringement if they met certain conditions.¹⁹⁵ The safe harbor requirements were also designed to weed out bad actors — service providers not acting in good faith, *i.e.*, those who intentionally or knowingly contribute to or profit from infringement and do nothing to remove the infringing content.¹⁹⁶ There are four separate safe harbor protections relating to ISPs engaging in the following activities: (1) transitory communications, (2) system caching, (3) information residing on systems at direction of users and (4) information location tools.¹⁹⁷ Section 512(c) is the safe harbor that file hosting services rely on for protection and therefore is the focus of this discussion.¹⁹⁸ Each safe harbor provision, including Section 512(c), has its own set of eligibility requirements, in addition to the general requirements applicable to all four of the safe harbors set out in Section 512(i). Below, we review how courts have interpreted the Section 512(c) requirements and discuss the import and overall implications for copyright owners seeking to hold file hosting services secondarily liable.

1. *Do File Hosting Services Fall Within Section 512(c)?*

The Section 512(c) safe harbor provides immunity to qualifying ISPs 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.”¹⁹⁹ As a preliminary matter, then, in

¹⁹⁵ See S. REP. NO. 105-190, at 8, 19, 48 (1998); H.R. REP. NO. 105-551, pt. 2, at 23 (1998). (“Title II [of the DMCA] preserves 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.”)

¹⁹⁶ *Id.*; see *Columbia Pictures v. Fung*, No. 06-5578, 2009 WL 6355911, at *17-18 (C.D. Cal. Dec. 21, 2009) (“[T]he statutory safe harbors are based on passive good faith conduct aimed at operating a legitimate internet business.”).

¹⁹⁷ 17 U.S.C. § 512 (2006).

¹⁹⁸ Only one case has ever been brought in which subsection (a) was asserted. In *Ellison v. Robertson*, the defendant AOL claimed protection under Section 512(a) for the safe harbor pertaining to transitory digital network communications or service providers acting as mere conduits. The court held that AOL’s fourteen-day period in which it stored and retained infringing material was “transient” and “intermediate” within the meaning of Section 512(a). 357 F.3d 1072, 1080-81 (9th Cir 2004). The court in *Field v. Google* held that Google’s cache for fourteen to twenty days was similar to the fourteen days considered transient in *Ellison* and was therefore protected under Section 512(b). 412 F. Supp. 2d 1106, 1124 (D. Nev. 2006).

¹⁹⁹ 17 U.S.C. § 512(c)(1) (2006) (emphasis added). The provision provides in pertinent part:

A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, 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, if the service provider . . .

order to fall under the Section 512(c) safe harbor, a file hosting service must “store” material at the direction of users and any covered allegedly infringing activities must occur “by reason of” the storage.

The act of hosting files necessarily includes storage. Most file hosting services, however, allow users to do more than merely store the files — they also allow users to share their files and many allow, and even encourage, users to make the files available to the public. Personal file storage services aimed at private individuals generally allow users to upload their files for personal backup and file access. Both of these services seem to fall squarely within “storage” or “by reason of storage.” If the user stores a file on a cloud service, he or she should be able to access those files. But the services also generally allow the user to share the files publicly; indeed, the default for many of these services is to make the uploaded files publicly available, even if users are allowed to designate that certain files be password-protected.²⁰⁰ As described above, some of the file hosting services, such as MP3tunes and Hotfile, are used in much the same manner as a peer-to-peer service, namely, to allow users to access infringing content for free and to further “share” infringing content with others. Incentives may be offered to users who upload content — especially popular content — such as providing additional bandwidth or reduced fees to those who upload content that is frequently downloaded by others.²⁰¹ At the same time, professional pirate sites use file hosting services to provide access to infringing copies of movies and music, for instance, by linking the users of their own Web sites back to files hosted on storage locker services, such as the recent Megaupload. This kind of piratical use of file hosting services generates an enormous amount of traffic through some of the major cloud “locker” services.²⁰²

Rights holders have argued that activities conducted by services to facilitate the unauthorized, infringing distribution, public performance and display of copyrighted content, such as making copies to convert files to

²⁰⁰ See *File hosting service*, WIKIPEDIA, http://en.wikipedia.org/wiki/File_hosting (last updated June 18, 2012 3:11 PM).

²⁰¹ For instance, Megaupload “offered an ‘Uploader Rewards’ Program, which promised premium subscribers transfers of cash and other financial incentives to upload popular works, including copyrighted works, to computer servers under the Mega Conspiracy’s direct control and for the Conspiracy’s ultimate financial benefit.” Indictment of Kim Dotcom, Megaupload Limited, et al. (E.D. Va.), Jan. 5, 2012.

²⁰² Megaupload is ranked 555 out of all Web sites for global traffic in the last month by Alexa. *Megaupload.com*, ALEXA, <http://www.alexa.com/siteinfo/megaupload.com> (last visited Apr. 26, 2012). RapidShare is visited even more frequently, ranking 154 for global traffic in the last month. *Rapidshare.com*, ALEXA, <http://www.alexa.com/siteinfo/rapidshare.com> (last visited Apr. 26, 2012).

other formats, playing back or streaming the content, and helping users locate the files through added functionality, are not “by reason of” storage and thus, are not covered by Section 512(c).²⁰³ They argue that a literal reading of the language of the statute, “by reason of storage,” does not encompass “making available” and other non-storage activities, and that content is not made available “by reason” of storing it. However, the case law to date has consistently rejected those arguments and held, to the contrary, that Section 512(c) covers all activities of file hosting services related to making content directly available to others through their services.²⁰⁴

In the recent Second Circuit decision, *Viacom International v. YouTube*, the court affirmed the district court, after requesting additional briefing on the issue (indicating it was not inclined to simply adopt the Ninth Circuit precedent), and held that (i) the conversion into standard display formats, (ii) the playback or streaming of videos on the “watch” page, and (iii) the “related videos” function that identifies thumbnails of related videos, were all activities that occurred “by reason of storage at the direction of the user.”²⁰⁵ The Second Circuit, however, remanded with respect to a fourth software function provided by YouTube, the syndication of the uploaded videos to third parties, including Verizon. The plaintiffs had argued “with some force”²⁰⁶ according to the court, that business transactions, such as syndication, do not occur at the “direction of the user.”²⁰⁷ The Second Circuit seemed to agree with this argument, but remanded to the district court to determine whether any of the videos in suit had been syndicated, to avoid “an advisory opinion on the outer boundaries of the storage provision.”²⁰⁸

The Second Circuit reasoned that, because (i) the definition of a service provider applicable to the Section 512(a) safe harbor prohibits the service provider from any modification of content passing through its system and (ii) that parallel limiting language is absent from the provisions applicable to Section 512(c), Congress must have intentionally omitted the limitation not to modify from Section 512(c). The court then concluded

²⁰³ See *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1146 (N.D. Cal. 2008).

²⁰⁴ See, e.g., *Perfect 10, Inc. v. CCBill, LLC*, 488 F.3d 1102, 1102 (9th Cir. 2007); *Viacom Int'l, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514 (S.D.N.Y. 2010), *rev'd and remanded in part and aff'd in part*, 676 F.3d 19 (2d Cir. 2012); *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 665 F. Supp. 2d 1099 (C.D. Cal. 2009); *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

²⁰⁵ 676 F.3d at 39-40. See also Court Order for Additional Briefing, *Viacom Int'l Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d. Cir. 2012).

²⁰⁶ *Viacom Int'l*, 676 F.3d at 40.

²⁰⁷ *Id.*

²⁰⁸ *Id.*

that since the prohibition against modification does not apply to Section 512(c), Section 512(c) “is clearly meant to cover more than mere electronic storage lockers.”²⁰⁹ While one might deduce from the absence of the “no modification” language, that a provider could modify the content under 512(c) and so could convert the user’s content to other formats for storage purposes, it is not at all “clear” how the ability to modify carries with it the ability to publicly perform, display or distribute the content.

The Ninth Circuit in *UMG Recordings v. Shelter Capital* similarly concluded that the Section 512(c) safe harbor covers all service provider functions conducted “for the purpose of facilitating access to user-stored material” and that file hosting service Veoh’s activities were covered under Section 512(c) because they occur “by reason of storage.”²¹⁰ The court held that Section 512(c) encompasses the access-facilitating processes that automatically occur when a user uploads a video to Veoh.²¹¹ It explained that Web hosting services “store user-submitted materials *in order to make those materials accessible* to other Internet users.”²¹² Equating “storage” with Web hosting, the court found that the generally-understood meaning of Web hosting includes making materials available and that a Web host that only stores materials for a single user and does not make it available to others, would be “more aptly described as an online back-up service.”²¹³ Finally, the court concluded that such a narrow reading of “by reason of storage” would create internal statutory conflict — because Section 512(c) codifies a detailed notice and takedown procedure by which service providers “disable access” to identified materials, the statute presupposes that service providers will provide access to users’ stored materials.²¹⁴

²⁰⁹ *Id.* at 39 (citing *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 620 F. Supp. 2d 1081, 1088 (C.D. Cal. 2008)).

²¹⁰ 667 F.3d 1022, 1031-35, 1050 (9th Cir 2011). In *UMG v. Shelter Capital*, the Ninth Circuit affirmed the district court’s summary judgment ruling in *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 620 F. Supp. 2d 1081 (C.D. Cal. 2008), that Veoh is entitled to safe harbor protection.

²¹¹ *UMG Recordings, Inc. v. Shelter Capital Partners*, 667 F.3d at 1031.

²¹² *Id.* at 1034.

²¹³ *Id.* at 1034. Note that cloud services such as those provided by Apple, Google and Amazon that allow a user to access his or her own content from anywhere do store materials for a single user.

²¹⁴ *Id.* at 1033 (citing 17 U.S.C. §512(c)(1)(A)(iii)). See also *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1146-48 (N.D. Cal. 2008) (a Web site for sharing user-submitted video content entitled to the Section 512(c) safe harbor when its users uploaded infringing media files). In *Io Group v. Veoh*, the district court relied heavily upon the legislative history of Section 512, which indicates that the storage covered by the statute is intended to include, by way of example, “providing server space for a user’s web site, for a chat room, or other forum in which material may be posted at the

Although it is difficult to imagine that Congress intended the phrase “by reason of storage” to include file sharing via file hosting, this issue appears to be a settled one especially with these recent decisions of the Second and Ninth Circuits. Thus, absent a Supreme Court ruling to the contrary, file hosting services that enable users to make infringing content available to the public likely will continue to be deemed protected under Section 512(c), provided, of course, that they comply with the specific requirements detailed below.

2. Section 512(c) Requirements

Once it is determined that the service provider falls within the general scope of the Section 512(c) safe harbor, it must show that it satisfies four additional requirements set out in Section 512(c) in order to qualify for protection.²¹⁵ The service provider must establish that it:

- Does not have actual knowledge that material on its network is infringing, or “awareness or facts or circumstances from which the infringing activity is apparent,”²¹⁶ and if it did obtain actual or apparent knowledge, that it acted “expeditiously to remove, or disable access to, the [infringing] material;”²¹⁷

direction of users.” *Id.* at 1146 (citing H.R. REP. 105-551, pt. 2, at 53 (1998)).

²¹⁵ Section 512(i) contains additional eligibility requirements that pertain to all of the four safe harbors, including that a service provider must (i) adopt a policy that provides for termination of service access by repeat infringers in appropriate circumstances, (ii) reasonably implement the policy, and (iii) inform users of the policy 17 U.S.C. § 512(i)(A) (2006). The scope of this requirement has also been a subject of much debate. In a number of cases where the service provider hosted rampant amounts of infringing content, plaintiffs have attempted to argue that this requirement has not been met, for the understandable reason that the file hosting services clearly have numerous repeat infringers who continue to use the service. Some of these cases have interpreted “reasonably implemented” to require only terminating accounts of blatant repeat infringers of whom the provider has been notified, generally by the rights holder. *See Perfect 10, Inc. v. CCBill, LLC*, 488 F.3d 1102, 1109 (9th Cir. 2007) (finding no genuine issue of material fact whether defendants prevented the implementation of their policies by failing to keep track of repeatedly infringing webmasters); *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d at 1143; *Capitol Records, Inc. v. MP3tunes, LLC*, 821 F. Supp. 2d 627, 638 (S.D.N.Y. 2011); *but see Flava Works, Inc. v. Gunter*, No. 10 C 6517, 2011 WL 3205399 (N.D. Ill. July 27, 2011).

²¹⁶ 17 U.S.C. § 512(c)(1)(A)(i)–(ii) (2006).

²¹⁷ *Id.* § 512(c)(1)(A)(iii).

- Does not receive a “financial benefit directly attributable” to any infringing activity that it maintains the right and ability to control;²¹⁸
- Has appointed a designated agent with the Copyright Office to receive notices of infringement;²¹⁹ and
- Has expeditiously removed or disabled access to material that is claimed to be infringing for which it has received appropriate notice through its designated agent.²²⁰

In recent years, the courts have construed these Section 512(c) eligibility requirements, particularly the “knowledge” requirement (in (1) above) and the “financial benefit and control” requirement (in (2) above), in an increasingly narrow manner — making it relatively easy for a service provider to qualify for the safe harbor. As a result, in some recent cases, courts have granted Section 512(c) immunity, even to service providers that were aware that infringement was rampant through the service and that were intentionally profiting from, or even dependent on, that infringing content for the success of the service. Below, this article describes how courts in recent cases have construed the actual knowledge and “red flag” awareness standards, as well as the right and ability to control and financial benefit standards.

a) Actual Knowledge and Red Flag Awareness

The actual knowledge and “red flag” awareness standards in subsection 512(c)(1)(A) have been avidly debated, including in the recent cases of *Viacom International v. YouTube*²²¹ and *UMG Recordings v. Shelter Capital*.²²² In order to qualify for the Section 512(c) safe harbor, a service provider must not have (1) “actual knowledge” that any activity or material on the service is infringing or (2) “awareness of facts or circumstances from which infringing activity is apparent” (referred to as “red flag” awareness).²²³ Further, if the provider acquires such knowledge or awareness, it must act expeditiously to remove or disable access to the material.²²⁴ A separate provision, Section 512(c)(1)(C), requires a service provider to comply with all takedown notices sent by copyright holders that meet the requirements set forth in Section 512(c)(3).

²¹⁸ *Id.* § 512(c)(1)(B).

²¹⁹ *Id.* § 512(c)(1)(C).

²²⁰ *Id.* § 512(c)(1)(C), 512(c)(2).

²²¹ 676 F.3d 19, 30-35 (2d Cir. 2012).

²²² 667 F.3d 1022, 1035-38, 1050 (9th Cir 2011).

²²³ 17 U.S.C. § 512(c)(1) (2006).

²²⁴ *Id.*

i) Specificity Requirement

Following earlier cases within the Ninth Circuit, the recent Second and Ninth Circuit decisions, *Viacom International v. YouTube* and *UMG Recordings v. Shelter Capital* respectively, held that the “actual knowledge” and “awareness” standards in subsection (c)(1) require knowledge of specific and identifiable infringements and that knowledge or awareness of infringing activity cannot otherwise be imputed — even if the service provider has general knowledge that the vast majority of content available through its site is infringing and does nothing to stop it.²²⁵ Thus, in the context of file hosting services, *both* actual knowledge *and* red flag awareness have been interpreted as knowledge or awareness of specific and identifiable infringements, as opposed to knowledge of infringing activity on the site generally, or even knowledge of rampant infringement. These courts have reasoned that, because a service provider with actual knowledge or red flag awareness may still be protected under Section 512 if it expeditiously removes the infringing material, such knowledge and awareness must include knowledge of the specific infringing copy and, by implication, its location; otherwise, the service provider could not remove it without having to search for it.²²⁶ Further, these courts have concluded that requiring a service provider to search for infringing content to remain protected would violate Section 512(m), which states that the Section 512 safe harbors are not conditioned on a service monitoring its service or affirmatively seeking facts regarding infringing activity.²²⁷ As the Second Circuit stated in *Viacom v. YouTube*, requiring expeditious removal in the absence of specific knowledge or awareness would create “an amorphous obligation to ‘take commercially reasonable steps’ in response to generalized awareness of infringement.”²²⁸

The Second and Ninth Circuits thus have held that the service provider can never be required to take any action to detect infringement, even a word or term search, or even to apply filtering software that it already possesses, because to do so would be inconsistent with Section 512(m). In so doing, they have expressly placed the burden to police in-

²²⁵ *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d at 30; *UMG Recordings, Inc. v. Shelter Capital Partners*, 667 F.3d at 1037-38; *see also Corbis*, 351 F. Supp. 2d at 1108-09; *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1148-49 (N.D. Cal. 2008); *Perfect 10, Inc. v. CCBill, LLC*, 488 F.3d 1102, 1114 (9th Cir. 2007).

²²⁶ *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d at 30-31; *UMG Recordings, Inc. v. Shelter Capital Partners*, 667 F.3d at 1037-38.

²²⁷ *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d at 35; *UMG Recordings, Inc. v. Shelter Capital Partners*, 667 F.3d at 1037-38.

²²⁸ *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d at 30-31.

fringement squarely on the copyright holder.²²⁹ We question whether rigidly applying the specificity requirement to services that blatantly host an overwhelming amount of infringing content leads to balanced law. For instance, the district court in *Viacom v. YouTube*, refused to find Section 512 “knowledge” on YouTube’s part and provided it with safe harbor protection, even though:

A jury could find that the defendants not only were generally aware of, but welcomed, copyright-infringing material being placed on their web-site. Such material was attractive to users, whose increased usage enhanced defendants’ income from advertisers . . .²³⁰

An issue related to the specificity requirement is the way courts have construed a Section 512(c) compliant takedown notice (i.e., one that triggers an ISP’s obligation to remove the content).²³¹ The consensus of the courts, including the lower courts in *UMG Recordings v. Veoh Networks* and *Viacom International v. YouTube*, is that to trigger an ISP’s takedown obligation, a notice must specify the precise location (item number, web address or URL) of the infringing copy of the work.²³² Further, courts generally have held that in response, an ISP must only remove that location-specific copy — not additional copies of the same work that may reside on the system.²³³ However, there does not appear to be any basis in the statute for requiring this level of specificity. Indeed, the notice provisions in the statute clearly envision that the rights owner might provide less specific information. Subsection (3)(iii) requires only information *reasonably sufficient* to permit the service provider to locate the material — not the precise location of each item of infringing content. Further, subsection (3)(ii) provides that “if multiple copyrighted works at a single on-line site are covered by a single notification, a *representative list* of such works at that site” suffices.²³⁴ The Fourth Circuit in *ALS Scan, Inc. v. RemarQ Communities, Inc.* noted:

²²⁹ See, e.g., *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d at 35; *UMG Recordings, Inc. v. Shelter Capital Partners*, 667 F.3d at 1037-38; *CCBill*, 488 F.3d at 1112-13 (defendant argued successfully that it could not identify which of the celebrity photos posted on its site were infringing (even though one of the sites was called “stolencelbritypics.com”)).

²³⁰ 718 F. Supp. 2d at 518.

²³¹ 17 U.S.C. § 512(c)(3) (2006)

²³² See *Viacom Int’l, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d at 528-29; *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 620 F. Supp. 2d 1081, 1109-10 (C.D. Cal. 2008); *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1089-92 (C.D. Cal. 2001); *Capitol Records, Inc. v. MP3tunes, LLC*, 821 F. Supp. 2d 627, 642-43 (S.D.N.Y. 2011). See also *CCBill*, 488 F.3d at 1112.

²³³ *Viacom Int’l, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d at 528-29; *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 665 F. Supp. 2d 1109-10.

²³⁴ 17 U.S.C. § 512(c)(3)(iii) (2006).

This subsection specifying requirements for notification does not seek to burden copyright holders with the responsibility of identifying every infringing work or even most of them — when multiple copyrights are involved. Instead, the requirements are written so as to reduce the burden of holders of multiple copyrights who face extensive infringement of their works.²³⁵

Despite the statutory language, courts generally have strictly construed the compliance requirements, narrowly construed the ISP's obligation to respond to takedown notices, and generally failed to imbue any meaning to the "representative list" language.²³⁶

In *Capitol Records v. MP3tunes*, the court gave the takedown notice slightly more teeth, by requiring MP3tunes to take down additional copies of the material identified in the notices that users had copied into their personal lockers.²³⁷ MP3tunes had removed infringing copies of which it received notice from its servers, but it had not removed copies of the same material (bearing the same hash number) made by users from the server copy and located in users' lockers.²³⁸ The court reasoned that MP3tunes could easily locate and remove those files since they bore the same hash tag, while the plaintiffs had no way to find the copies stored in users' "lockers" and identify them.²³⁹ The court's determination that MP3tunes, in responding to takedown notices, is also required to remove additional copies from their customers' lockers represents somewhat of a departure from prior decisions, discussed above, which have very narrowly construed an ISP's obligation to respond to takedown notices. This strict and narrow construction stems from steadfast judicial interpretation of Section 512(m) to preclude any burden being placed on the ISP to search for or locate infringing materials.²⁴⁰ The *MP3tunes* ruling regarding locker copies, however, represents an acknowledgement that in certain instances, it will

²³⁵ 239 F.3d 619, 625 (4th Cir. 2001); *see also* Perfect 10, Inc., v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1180 (C.D. Cal. 2002) (noting that Cybernet's refusal to allow such a representative list upsets the "Congressionally apportioned burden between copyright hold and service provider by placing the entire burden on the copyright owner.").

²³⁶ *See* Viacom Int'l, Inc. v. YouTube, Inc., 718 F. Supp. 2d at 528-29; UMG Recordings, Inc. v. Veoh Networks, Inc., 665 F. Supp. 2d 1110 (merely providing an artist's name is not information reasonably sufficient to permit the service provider to locate the material under Section 512(c)(3)); *Capitol Records, Inc. v. MP3tunes, LLC*, 821 F. Supp. 2d at 642-43; *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1089-92 (C.D. Cal. 2001) (informing eBay that counterfeit copies of the film *Manson* were being offered for sale was insufficient under Section 512(c)(3)).

²³⁷ 821 F. Supp. 2d at 642-43.

²³⁸ *Id.*

²³⁹ *Id.*

²⁴⁰ *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 665 F. Supp. 2d 1109-10.

be impossible for the copyright owner to identify all infringing copies and that an ISP can in fact have greater knowledge and ability to locate infringing materials.

Below, we describe how Section 512(c) came to be interpreted to protect services flagrantly hosting infringing content and why, in terms of maintaining the balance between protecting copyright and encouraging innovation, that may not be the most accurate or beneficial interpretation of section 512(c). We look at actual knowledge and red flag awareness standards, in turn.

ii) Actual Knowledge

To determine what Congress intended by use of the term “knowledge,” the basic principles of statutory construction tell us that instead we should look to the meanings already ascribed to it in the relevant common law,²⁴¹ i.e., the case law regarding contributory liability in copyright infringement. As described above, knowledge of the infringing activity is an essential element of traditional contributory liability.²⁴² According to traditional contributory liability case law, knowledge that infringement is actually occurring is sufficient — knowledge of each specific item of infringing material is *not* necessary, however, to find liability. For instance, in *Fonovisa*, the swap meet operator knew there were vendors selling infringing music tapes, but he could not have told you which tapes exactly were being sold at which booths.²⁴³

The *Napster* court found that Napster had both actual and constructive knowledge based on an internal Napster document uncovered in discovery that demonstrated its knowledge that the site was being used for infringement of sound recordings, the sophistication of the Napster executives and the fact that the RIAA had advised Napster of more than 12,000 infringing files, some of which were still available.²⁴⁴ The court drew an important distinction between the case (1) in which a service provider learns of specific infringing material available on its site and “fails to purge

²⁴¹ *Perfect 10, Inc. v. CCBill, LLC*, 488 F.3d 1102, 1117 (9th Cir. 2007) (“Based on the ‘well-established rule of construction that where Congress uses terms that have accumulated settled meaning under common law, a court must infer, unless the statute otherwise dictates, that Congress means to incorporate the established meaning of those terms.’” (quoting *Rossi v. Motion Pictures Ass’n of Am.*, 391 F.3d 1000, 1004 n.4 (9th Cir. 2004) (quoting *Neder v. United State*, 527 U.S. 1, 21 (1999))); *see also* *F.D.I.C. v. Meyer*, 510 U.S. 471, 476 (1994) (holding that in the absence of a specific statutory definition, a statutory term is construed “in accordance with its ordinary or natural meaning”).

²⁴² *See supra* Section III.1.a.

²⁴³ *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 264 (9th Cir. 1996).

²⁴⁴ *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1021 (9th Cir. 2001).

such material from its system,”²⁴⁵ and (2) where the structure of the service provider’s system merely “allows for the exchange of copyrighted material,”²⁴⁶ with the latter not constituting actual knowledge.

Similarly, courts have found that peer-to-peer service providers that actually knew there was massive infringement occurring on their services were not required to have knowledge of each infringing item to give rise to contributory infringement. In *Arista Records v. Usenet.com*, the court expressly stated that knowledge of specific infringements is *not* required to support a finding of contributory infringement and found that it was “beyond purview” that the defendants knew or should have known of infringement by their users and that their services were used primarily to obtain copyrighted material.²⁴⁷ Nor did the Court in *Grokster* require knowledge of specific infringements; the fact that the *Grokster* defendants were intentionally encouraging or inducing users to infringe was sufficient.²⁴⁸ In *Aimster*, the court found the defendants had culpable knowledge where they willfully blinded themselves to infringement generally by using encryption technology.²⁴⁹

Courts in the Ninth Circuit were some of the first to analyze knowledge requirements in the Section 512(c)(1)(A) context, and the case law requiring item-specific knowledge quickly developed. In several cases, the courts required particular knowledge of specific infringements of the nature that one would obtain from a DMCA takedown notice. In each of *Perfect 10 v. CC Bill*, *Corbis v. Amazon.com*, *Io Group v. Veoh Networks* and *UMG Recordings v. Veoh Networks* (later affirmed by *UMG Recordings v. Shelter Capital*), the fact that the plaintiffs had failed to provide compliant DMCA notices prior to the commencement of the lawsuit was an important factor weighing against a finding of actual knowledge.²⁵⁰

²⁴⁵ *Id.* at 1021 (citing *Religious Tech. Ctr. v. Netcom On-Line Commc’n Servs., Inc.*, 907 F. Supp. 1361, 1374 (N.D. Cal. 1995)).

²⁴⁶ *Id.* (citing *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 442-43 (1984)).

²⁴⁷ 633 F. Supp. 2d 124, 124 (S.D.N.Y. 2009); *see also* *Arista Records, LLC v. Lime Group, LLC*, No. 06 Civ. 5936, 2010 WL 2291485 (S.D.N.Y. May 25, 2010).

²⁴⁸ *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 923-24 (2005) (“It is uncontested that [Grokster and StreamCast] are aware that users employ their software primarily to download copyrighted files, even if the decentralized FastTrack and Gnutella networks fail to reveal which files are being copied, and when.”). *Id.* at 940 (“The unlawful objective is unmistakable.”).

²⁴⁹ *In re Aimster Copyright Litigation*, 334 F.3d 643, 655 (7th Cir. 2003).

²⁵⁰ *Corbis*, 351 F. Supp. 2d 1090, 1107-08 (W.D. Wash. 2004); *Perfect 10, Inc. v. CCBill, LLC*, 488 F.3d 1102, 1111-12 (9th Cir. 2007); *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1136 (N.D. Cal. 2008); *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 620 F. Supp. 2d 1081, 1104 (C.D. Cal.

The Ninth Circuit in *CC Bill* expressly stated that actual knowledge would not be imputed to the defendant CC Bill because it had not received compliant DMCA notices.²⁵¹ This view was reflected in the *Io Group v. Veoh Networks*²⁵² and *UMG Recordings v. Veoh Networks*,²⁵³ district court decisions in the Northern and Central Districts of California, respectively. The Southern District of New York followed suit in *Viacom v. YouTube*,²⁵⁴ *Wolk v. Kodak Imaging Network*²⁵⁵ and, to an extent, *Capitol Records v. MP3tunes*.²⁵⁶

The district court in *UMG Recordings v. Veoh Networks* found that the defendant lacked actual knowledge for purposes of Section 512(c)(1)(A) despite the fact that Veoh (i) knew it was hosting an entire category of copyrighted music, while knowing it had no licenses for such content; (ii) had tagged more than 240,000 videos as music videos, which again it knew it had no licenses for; (iii) paid search engines to appear in search results for terms that included UMG music; (iv) based on the evidence presented, founders, employees and investors admittedly knew of widespread infringement; all while (v) Veoh delayed use of fingerprinting technology that it possessed and could have easily used to search indexes to locate infringing content.²⁵⁷ The district court in *Io Group v. Veoh Networks* similarly held that Veoh had no “knowledge” despite similar facts.²⁵⁸

The Ninth Circuit affirmed the district court in *UMG Recordings v. Shelter Capital*. It found that UMG had not sent Veoh any takedown notices, which the court explained, “stripped it of the most powerful evidence of a service providers’ knowledge — actual notice of infringement from the copyright holder.”²⁵⁹ Notably, the Ninth Circuit readily dismissed UMG’s arguments that because Veoh had no licenses from major music owners and knowingly hosted an entire category of copyrighted content — namely music — Veoh had actual knowledge sufficient to disqualify it from safe harbor protection.²⁶⁰ The court adopted Veoh’s argument that some of the music might legally appear on the service, including

2008); *UMG Recordings, Inc. v. Shelter Capital Partners*, 667 F.3d 1022 (9th Cir. 2011).

²⁵¹ 488 F.3d at 1112-13.

²⁵² 586 F. Supp. 2d at 1136.

²⁵³ 665 F. Supp. 2d at 1104.

²⁵⁴ 718 F. Supp. 2d at 524.

²⁵⁵ No. 10-4135, 2012 WL 11270 at *5 (S.D.N.Y. 2012).

²⁵⁶ 821 F. Supp. 2d 627, 642-43 (S.D.N.Y. 2011).

²⁵⁷ 665 F. Supp. 2d at 1108-09.

²⁵⁸ 586 F. Supp. 2d at 1148.

²⁵⁹ 667 F.3d 1022, 1036 (9th Cir 2011).

²⁶⁰ *Id.* at 1036-39.

videos that users created and some that Veoh had obtained through arrangements with copyright holders.²⁶¹ The court explained that if:

merely hosting material that falls within a category of content capable of copyright protection, with the general knowledge that one's services could be used to share unauthorized copies of copyrighted material, was sufficient to impute knowledge to the service providers, the Section 512(c) safe harbor would be rendered a dead letter.²⁶²

Further, the Ninth Circuit stated that notice and takedown procedures were made available to rights holders as part of the DMCA's attempt to foster cooperation between copyright holders and service providers, and that copyright holders are in a better position to identify infringing copies since they know exactly what they own.²⁶³ Under Section 512(c)(3)(B), a deficient takedown notice "shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent."²⁶⁴ The Ninth Circuit went one step further and held that actual knowledge can only come from the copyright owner and that it must be in the form of a proper Section 512(c) takedown notice.²⁶⁵ The court reasoned that other sources of potential knowledge could only constitute red flag knowledge, at most, not actual knowledge, because the service provider "would have no assurance that a third party who does not hold the copyright in question could know whether the material was infringing."²⁶⁶ In other words, only the copyright holder can know for certain if the particular copy is infringing and provide notice that constitutes actual knowledge. Because that notice must be in the form of a DMCA complaint takedown notice, according to the Ninth Circuit's logic, there is no way to acquire actual knowledge other than by a compliant DMCA notice. Hence, the Ninth Circuit effectively collapsed the actual knowledge standard into the notice and takedown requirement, rendering the former superfluous.

²⁶¹ *Id.* at 1038-39.

²⁶² *Id.* at 1036-37.

²⁶³ *Id.* at 1037.

²⁶⁴ *Id.* (citing 17 U.S.C. §512 (c)(3)(B) (2006)).

²⁶⁵ *Id.* at 1040; *id.* at n.14. UMG argued that an email sent from the CEO of Disney to Veoh investor Michael Eisner regarding specific copyrighted Disney content on the service constituted actual or red flag knowledge. The court noted that Disney, as a copyright holder, was subject to the notification requirements of Section 512(c)(3). It further stated that, even if the notice came from a third party, "it would not be obvious how Veoh's awareness of apparent infringement of Disney's copyrights over movies and television shows would advance UMG's claims that Veoh hosted unauthorized UMG music videos." *Id.* at n.13.

²⁶⁶ *Id.* at n.14.

The district court in *Viacom International v. YouTube* was the first court outside of the Ninth Circuit to expressly state that actual knowledge under Section 512(c)(1)(A) means knowledge of “specific and identifiable” copies of infringing content, including the location of each such copy.²⁶⁷ The district court in *Viacom* suggested that the only evidence of actual knowledge that a plaintiff could proffer that would disqualify a defendant from the safe harbor would be by virtue of having received a fully compliant DMCA takedown notice — one that included identification of each specific item of infringing content and its specific location, e.g., its URL.²⁶⁸ The court found that YouTube had no knowledge of infringement other than through DMCA notices with which it complied, despite evidence in the record that the founders knew that 70-80% of the content on the site was infringing and expressly discussed the need to keep certain infringing items on the site in order to attract more views.²⁶⁹

The district court in *Capitol Records v. MP3tunes* adopted the *Viacom* district court’s interpretation of Section 512(c) and refused to impute actual knowledge of any infringement to MP3tunes unless it had received an effective takedown notice which identified the infringing content.²⁷⁰ Following on the heels of *MP3Tunes*, in *Wolk v. Kodak Imaging Network*, a photographer alleged copyright infringement based on the fact that unauthorized copies of her photographs were uploaded to the Photobucket site.²⁷¹ The court found that Photobucket had complied with notice and takedown by removing all identified copies and that to hold Photobucket responsible for any infringement other than that which it received specific notice would be akin to requiring Photobucket to “police its site to uncover current infringements and prevent future infringements” — which would be a burden “beyond what is required under the DMCA.”²⁷²

²⁶⁷ 718 F. Supp. 2d 514, 528 (S.D.N.Y. 2010), *rev’d and remanded in part and aff’d in part*, 676 F.3d 19 (2d Cir. 2012).

²⁶⁸ *Id.*; *see also* *Wolk v. Kodak Imaging Network, Inc.*, 2012 WL 11270, at *5 (S.D.N.Y. 2012); *Perfect 10, Inc. v. CCBill, LLC*, 488 F.3d 1102, 1113 (9th Cir. 2007); *Hendrickson v. Amazon.com*, 298 F. Supp. 2d at 914, 915 (C.D. Cal. 2003); *but see* *Perfect 10, Inc., v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1169-70 (C.D. Cal. 2002). In *Hendrickson v. eBay*, the court found that the defendant could not be imputed with knowledge where the plaintiff’s notice did not specify the eBay item number that would enable the defendant eBay to identify the content. 165 F. Supp. 2d 1082, 1090 (C.D. Cal. 2001).

²⁶⁹ The district court in *Viacom* concluded that “[g]eneral knowledge that infringement is ‘ubiquitous’” does not impose a duty on the service provider to monitor or search its service for infringements.” 718 F. Supp. 2d at 525.

²⁷⁰ 821 F. Supp. 2d 627, 642-43 (S.D.N.Y. 2011).

²⁷¹ 2012 WL 11270 at *5.

²⁷² *Id.* at *5.

The Second Circuit in the recent *Viacom International v. YouTube* decision agreed with the district court that actual (and red flag) knowledge means “knowledge or awareness of specific infringing material.”²⁷³ In analyzing whether actual knowledge could mean general knowledge or had to be specific, the court decided it must be the latter because Section 512(c) would otherwise be internally inconsistent. To qualify for protection, the provider has the obligation to take such material down expeditiously upon obtaining such knowledge or awareness. The court explained that “expeditious removal is possible only if the service provider knows with particularity which items to remove.”²⁷⁴ Because there was evidence that YouTube employees had knowledge of specific Viacom-owned clips and made decisions not to take the infringing materials down, the Second Circuit reversed and remanded on whether there was a genuine issue of material fact as to YouTube’s specific knowledge of infringing copies of the Viacom works in-suit.²⁷⁵

The record evidence relied upon by the Second Circuit included a YouTube founder’s report noting the availability on the service of well-known Viacom-owned shows, e.g., *South Park* and the *Daily Show*, and further stating that “although YouTube is not legally required to monitor content . . . and complies with DMCA takedown requests, we would benefit from *reemptively* removing content that is blatantly illegal and likely to attract criticism.”²⁷⁶ The record also included incriminating internal YouTube e-mails showing knowledge or awareness that specific content was being offered on YouTube without authorization from the copyright owners (i.e., Bud Light commercials, CNN shuttle clip) — these e-mails also evidenced a desire to keep the popular copyrighted content up until YouTube was “bigger and better known.”²⁷⁷

The Second Circuit departed from the Ninth Circuit’s view of actual knowledge in two important respects. First, it acknowledged that there might be instances of actual knowledge obtained from sources other than DMCA takedown notice, i.e., YouTube’s own internally-generated knowledge.²⁷⁸ Second, as discussed in more detail below, the Second Circuit distinguished the actual knowledge from the red flag awareness standard

²⁷³ *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 26 (2d Cir. 2012).

²⁷⁴ *Id.* at 30.

²⁷⁵ *Id.* at 34.

²⁷⁶ *Id.* at 33.

²⁷⁷ *Id.* at 33-34. For instance, regarding the CNN space shuttle clip, one of the YouTube founders stated in an e-mail, “the CNN space shuttle clip, I like. We can remove it once we’re bigger and better known, but for now that clip is fine.” And regarding the Bud Light commercials, a founder stated also in an e-mail: “can we please leave these in a bit longer? Another week or two can’t hurt.”

²⁷⁸ *Id.* at 31.

by explaining that actual knowledge was subjective specific knowledge while the latter was an objective standard for specific knowledge.²⁷⁹ The court explained that “actual” knowledge denotes a subjective belief, while “red flag” knowledge refers to an objective, reasonableness standard.²⁸⁰

iii) Red Flag Awareness

The courts in the recent Second and Ninth Circuit Section 512(c) cases have also narrowly interpreted the “red flag” standard in Section 512(c)(1)(A), almost equating it to the actual knowledge standard by requiring awareness of specific items of infringing material. Red flag awareness — where a service provider is aware of facts and circumstances from which infringement is apparent — is somewhat similar to the “constructive knowledge” standard for a finding of contributory liability. Under the common law, constructive knowledge is found where the defendant “should have known” of the infringement and includes “willful blindness.”²⁸¹ The test for red flag awareness appears to be somewhat higher than the constructive knowledge standard of “should have known.” It has been described as: “whether the service provider *deliberately proceeded in the face of blatant factors* of which it was aware.”²⁸² The legislative history describes the standard in Section 512(c)(1)(A) as follows:

Subsection (c)(1)(A)(ii) can best be described as a ‘red flags’ test. As stated in subsection (1), a service provider need not monitor its service or affirmatively seek facts indicating infringing activity [], in order to claim this limitation on liability (or, indeed any other limitation provided by the legislation). *However, if the service provider becomes aware of ‘red flags’ from which infringing 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.²⁸³

In connection with the Section 512(d) safe harbor (which contains an identical “red flag” knowledge standard), Congress noted that “a service provider would have no obligation to seek out copyright infringement, but it would not qualify for the safe harbor if it had turned a blind eye to ‘red flags’ of obvious infringement.”²⁸⁴ In other words, if it should be evident to a service provider that there is infringing content on its site, it should not be able to shield itself from liability under Section 512 any more than a contributory infringer should be able to feign lack of knowledge by pur-

²⁷⁹ *Id.*

²⁸⁰ *Id.*

²⁸¹ See *In re Aimster Copyright Litigation*, 334 F.3d 643, 649 (7th Cir. 2003); see *supra* Section III.1.d.

²⁸² *Corbis*, 351 F. Supp. 2d at 1108-09.

²⁸³ S. REP. NO. 105-190, at 44 (1998) (emphasis added).

²⁸⁴ *Id.* at 48 (emphasis added); see also *id.* (giving examples of “red flags” as the use of names such as “pirate” and “bootleg”).

posely trying to hide its head in the sand.²⁸⁵ As Congress stated, when “the infringing nature” of the site “would be apparent from even a brief and casual viewing, safe harbor status . . . would not be appropriate.”²⁸⁶ The legislative history makes it clear that where there are signs of obvious infringement, the service provider must take some action to locate it and remove it: “Once one becomes aware of such infringement . . . one may have an obligation to check further.”²⁸⁷

Despite the legislative history, numerous courts (e.g., *Perfect 10 v. CC Bill*, *UMG Recordings v. Shelter Capital*, *Io Group v. Veoh Networks*, *Viacom v. YouTube*, *Capitol Records v. MP3tunes* and *Wolk v. Kodak Imaging*) have adopted the view, to varying degrees, that a service provider should have no obligation to make any investigation of infringement even if it is blatantly obvious that the site is mainly being used for infringement. Even where the cases cite to statements in the legislative history, such as that “apparent knowledge requires that the service provider deliberately proceeded in the face of blatant factors of which it was aware” or “turned a blind eye to ‘red flags’ of obvious infringement,”²⁸⁸ they each failed to find “red flag” knowledge on the grounds that the service provider would have had to take some action — even just a text or index search of its system — to locate the infringing activity.²⁸⁹

Notably, in *Perfect 10, Inc. v. CCBill, LLC*, the Ninth Circuit held that providing services to Web sites named “illegal.net” and “stolencelebrities.com” was not enough to raise a ‘red flag’ — even though, as described above, the legislative history provides as examples of “red flags” the use of analogous names such as “pirate” and “bootleg.”²⁹⁰ In *Io Group v. Veoh Networks*, the court found that awareness of professional quality videos containing Io’s trademark did not constitute red flags.²⁹¹ The district court in *UMG Recordings v. Veoh Networks* maintained that, even if Veoh’s “founders, employees, and investors knew that widespread

²⁸⁵ See *Aimster*, 334 F.3d at 655; *Columbia Pictures Indus., Inc. v. Fung*, No. 06-5578, 2009 WL 6355911, at *21-22 (C.D. Cal. Dec. 21, 2009); see *supra* Section III.1.d.

²⁸⁶ H.R. REP. NO. 105-551, pt. 1, at 26 (1998).

²⁸⁷ *Id.*

²⁸⁸ *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1148 (N.D. Cal. 2008); see also *Corbis*, 351 F. Supp. at 1108.

²⁸⁹ See, e.g., *UMG Recordings, Inc. v. Shelter Capital Partners*, 667 F.3d 1022, 1031-39 (9th Cir 2011).

²⁹⁰ 488 F.3d 1102, 1113 (9th Cir. 2007); but see *Playboy Enters., Inc. v. Webworld, Inc.*, 991 F. Supp. 543, 553-53 (N.D. Tex. 1997) (finding infringement and remarking that “a newsgroup named, for example, ‘alt.sexy.playboy’ or ‘alt.mag.playboy’ might instantly be perceived as problematic from the standpoint of federal copyright law”).

²⁹¹ 586 F. Supp. at 1148-49.

infringement was occurring on the Veoh system,” such “general awareness of infringement, without more” is not enough to constitute “red flag” knowledge.²⁹² In *UMG Recordings v. Shelter Capital*, the Ninth Circuit agreed with the district court’s understanding of red flag awareness, stating that the district court had “properly followed our analysis in *CCBill*, which reiterated that the burden remains with the copyright holder rather than the service provider.”²⁹³ The Ninth Circuit also agreed that the none of the following could be considered red flags: news articles from major media articles describing Veoh as a haven for pirated content, including acknowledgements in the press from Veoh’s CEO that it was hosting infringing content, an e-mail from Disney’s CEO complaining that Disney properties were available on Veoh without authorization, e-mail from a user that there was plenty of copyright infringing material available on Veoh.²⁹⁴

The district court in *Viacom* relied in part on the district court’s decision in *UMG Recordings v. Veoh Networks*, including the statement: “CCBill teaches that if investigation of ‘facts and circumstances’ is required to identify material as infringing, then those facts and circumstances are not ‘red flags.’”²⁹⁵ Although the court found that infringement on the site was ubiquitous, it also did not find any red flags of infringement. The district court stated that: “General knowledge that infringement is ‘ubiquitous’ does not impose a duty . . . to monitor or search its services for infringement.”²⁹⁶

The Second Circuit in *Viacom* affirmed the district court’s holding that red flag awareness of “facts and circumstances from which infringing activity is apparent” requires awareness of specific infringing activity.²⁹⁷ It agreed that ubiquitous infringement on a service is insufficient to constitute a red flag that would disqualify a service provider.²⁹⁸ Viacom argued that requiring item-specific knowledge under both red flag awareness and actual knowledge rendered the red flag provision superfluous.²⁹⁹ While acknowledging that it is required to “disfavor interpretations of statutes that render language superfluous,” the court distinguished actual and red

²⁹² 620 F. Supp. 2d 1081, 1109 (C.D. Cal. 2008).

²⁹³ 667 F.3d at 1038.

²⁹⁴ *Id.* at 1035-41.

²⁹⁵ *Viacom Int’l, Inc., v. YouTube, Inc.*, 718 F. Supp. 2d 514, 525 (S.D.N.Y. 2010), *rev’d and remanded in part and aff’d in part*, 676 F.3d 19 (2d Cir. 2012) (citing *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 665 F. Supp. 2d at 1108).

²⁹⁶ *Id.* at 525.

²⁹⁷ *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d at 31-32.

²⁹⁸ *Id.* at 33.

²⁹⁹ *Id.* at 31.

flag knowledge on grounds other than specificity.³⁰⁰ As mentioned, the court drew a distinction between actual and red flag knowledge on the basis that “actual” knowledge denotes a subjective belief, while “red flag” knowledge refers to an objective, reasonableness standard.³⁰¹ The court further explained that actual knowledge means the service provider itself in fact knew of a specific infringing item, while red flag knowledge depends on whether the provider was subjectively aware of facts and circumstances that would cause a reasonable person, under an objective standard, to know of the specific infringing item.³⁰² Given the record evidence that YouTube was aware of specific Viacom-owned clips, the court also reversed and remanded on the issue of red flag awareness.³⁰³ The court stated: “On these facts, a reasonable juror could conclude that YouTube had actual knowledge of specific infringing activity, or was at least aware of facts or circumstances from which specific infringing activity was apparent.”³⁰⁴

The Second Circuit in *Viacom* failed to provide any concrete details or examples as to what would constitute a red flag under this framework that would not also be actual knowledge. And it is difficult to envision a scenario in which this distinction would create any difference as a practical matter — where a service provider might be aware of facts and circumstances from which it is apparent that a particular copy of infringing content is available at a specific online location on its service and yet not have actual knowledge of that copy. In *UMG Recordings v. Shelter Capital*, upon UMG’s petition for rehearing and rehearing *en banc*, the Ninth Circuit has asked the parties to submit supplemental briefs on the Second Circuit’s distinction between red flag and actual knowledge. As a result, there may be more guidance on this issue from the Ninth Circuit in the near future.³⁰⁵

As another point of distinction from the *UMG Recordings v. Shelter Capital* case, the Viacom court explicitly considered the role of willful ig-

³⁰⁰ *Id.*

³⁰¹ *Id.*

³⁰² *Id.* But see S. REP. NO. 105-190, at 44 (1998) (stating that red flag test “has both a subjective and an objective element”).

³⁰³ *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d at 34.

³⁰⁴ *Id.*

³⁰⁵ On June 7, 2012, the court in *UMG v. Shelter Capital* on a petition for a rehearing *en banc* requested from the parties for a supplementary brief on whether (i) the Second Circuit drew the right distinction between actual and red flag knowledge and whether it affects the disposition of the case and (ii) whether the right and ability to control disqualifier in Section 512(c)(1)(B) requires knowledge of specific infringing material. See Court Order, *UMG Recordings, Inc. v. Shelter Capital Partners*, No. 2:07-cv-05744 (9th Cir. June 7, 2012).

norance and agreed with the plaintiff that willful ignorance could in some instances be red flag knowledge. It conditioned willful blindness on Section 512(m), however, stating that willful blindness cannot require “an affirmative duty to monitor” or investigate to be eligible for the safe harbor. It defined “willful blindness” as awareness of a “high probability of the fact in dispute and consciously avoiding confirming that fact.”³⁰⁶ If Section 512(m) prohibits *any* requirement to look for infringing content, as the Second and Ninth Circuits have held, then again, from a practical standpoint, it’s not clear under what circumstances an internet service provider might deliberately avoid guilty knowledge of specific acts of infringement without having first conducted any investigation of specific facts. For example, in *Aimster*, the defendants were willfully blind to infringement on the site generally, not to specific infringements. In order to encrypt particular items of infringement in order to blind themselves to them, the defendants would have had to know of the specific infringements or at least their location.

In the context of peer-to-peer services, courts have disqualified the service provider from Section 512 protection based on a finding of willful ignorance or blindness of infringement generally. In the summary judgment context, the *Fung* court found that over 90–95% of the content available to U.S. users was infringing and that the site was designed to make it easy to find popular movies and television shows, none of which were licensed. The *Fung* court stated: “in light of this overwhelming evidence, the only way Defendants could have avoided knowing about their users’ infringement is if they engaged in ‘ostrich-like refusal to discover the extent to which their systems were being used to infringe copyright.’”³⁰⁷ The court in *Fung* added: “inducement liability and the [DMCA] safe harbors are inherently contradictory. The statutory safe harbors were intended to protect passive, good faith conduct aimed at operating a legitimate internet business, while inducement liability is based on active bad faith conduct aimed at promoting infringement.”³⁰⁸ This seems fairly straightforward — one should not be able to intentionally induce infringement and then throw one’s hands up in ignorance. That would amount to the type of culpable willful blindness described in *Aimster*.

In *Aimster*, Judge Posner did not directly address red flag knowledge, but denied safe harbor protection on the grounds that a service provider could not shield itself from liability by willful ignorance. Consistent with the legislative history and the statute itself, Judge Posner interpreted the safe harbors generally as requiring a service provider to take action where

³⁰⁶ *Viacom Int’l, Inc. v. YouTube, Inc.*, 376 F.3d at 35.

³⁰⁷ *Columbia Pictures v. Fung*, No. 06-5578, 2009 WL 6355911, at *17-18 (C.D. Cal. Dec. 21, 2009).

³⁰⁸ *Id.* at *22.

reasonable — when it is in a better position to do so than the rights holder. He succinctly summed up the Section 512 requirements in one paragraph, explaining:

The common element of the safe harbors is that the service provider must do what it can reasonably be asked to do to prevent the use of its service by repeat infringers. 17 U.S.C. 512 (i)(1)(A). Far from doing anything to discourage repeat infringers . . . Aimster invited them to do so, showed them how they could do so. . . and disabled itself from doing anything to prevent infringement.³⁰⁹

The *Fung* and *Aimster* decisions each involved clearly bad actors providing peer-to-peer services; and in none of them was specific knowledge required. The courts refused to provide safe harbor protection to clearly culpable defendants.³¹⁰

The Second Circuit in *Viacom* appeared somewhat troubled by the clear knowledge and awareness of infringement that the YouTube founders displayed in the record (during the period in suit — approximately 2005-2008). Although it agreed that general awareness of infringement can never be disqualifying knowledge under Section 512, it created a couple of important nuances, including the subjective/objective knowledge distinction discussed above, and the recognition that willful blindness could amount to knowledge or awareness under Section 512(c).³¹¹

b) Right and Ability to “Control” Infringing Activity and Direct Financial Benefit

Under Section 512(c)(1)(B), a service provider is entitled to safe harbor protection if it “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.”³¹² Thus, a service provider will be excluded from the safe harbor if it has “the right and ability to control the infringing activity” and “receives a financial benefit directly attributable to [the infringing] activity.”³¹³ The language of Section 512(c)(1)(B) directly tracks the elements of common law vicarious liability.³¹⁴ Both el-

³⁰⁹ *In re Aimster Copyright Litigation*, 334 F.3d 643, 655 (7th Cir. 2003).

³¹⁰ The *Fung* decision, however, is on appeal, and the appellate court could be waiting for a final decision in *Shelter Capital* before rendering a decision. See U.S. Court of Appeals for the Ninth Circuit, Docket No. 10-55946.

³¹¹ See *supra* Section III.3.b(i); see also *Viacom Int’l v. YouTube, Inc.*, 676 F.3d at 35.

³¹² 17 U.S.C. § 512(c)(1)(B) (2006).

³¹³ *Id.* § 512(c)(1)(B).

³¹⁴ In discussing the vicarious liability standard, the Supreme Court and this *Viacom* court have used the language “right and ability to control” and “right and ability to supervise” interchangeably. See *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 930 n.9 (2005) (stating

ements — the right and ability to control *and* the direct financial benefit — must be established in order to deny a defendant's immunity under Section 512(c).

i) Ability to Control Infringing Activity

As described above, under well-established rules of statutory construction, the common law understanding of the standard should be applied.³¹⁵ Nevertheless, the cases have interpreted the “right and ability to control” standard somewhat more strictly in the Section 512 context than the vicarious liability standard on which it was based.³¹⁶ In vicarious liability cases, courts have found that the ability to exclude users from the system and terminate their accounts was sufficient to demonstrate the right and ability to control for purposes of establishing vicarious liability.³¹⁷ Recent Section 512 cases, however, have stated that “something more” than the ability to terminate users' accounts is required in the 512 context — without defining what that “something more” is.³¹⁸ The rationale is that in order to be eligible for Section 512, a service provider must have the ability to take infringing material down, and so this requirement cannot mean that if it does have that ability it is not eligible.

In *Corbis v. Amazon.com*, for instance, the court found that Amazon did not have the right and ability to control infringing activity on its third-

that a vicarious liability theory “allows imposition of liability when the defendant profits directly from the infringement and has a right and ability to supervise the direct infringer”); *see also* H.R. REP. NO. 105-551 (Part 1) at 25-26 (emphasis added) (“The financial benefit standard in subparagraph (B) is intended to codify and clarify the direct financial benefit element of vicarious liability. . . . The “*right and ability to control*” language in subparagraph (B) codifies the second element of *vicarious liability*.”).

³¹⁵ *See* Perfect 10, Inc. v. CCBill, LLC, 488 F.3d 1102, 1117 (9th Cir. 2007).

³¹⁶ *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1150 (N.D. Cal. 2008); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1181 (C.D. Cal. 2002); *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1094 (C.D. Cal. 2001); *CoStar Group, Inc. v. LoopNet, Inc.*, 164 F. Supp. 2d 688, 704 (D. Md. 2001); *see also* *Viacom Int'l, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d at 527 (stating that because YouTube lacked knowledge of the specific location of infringing material it could not control the infringement; however, this contradicts one of the longstanding attributes of vicarious liability that knowledge is not a required element).

³¹⁷ *See, e.g.*, *A&M Records, Inc. v. Napster*, 239 F.3d 1004, 1023 (9th Cir. 2001); *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1173 (9th Cir. 2007) (holding that, consistent with *Grokster*, a service provider “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”).

³¹⁸ *See, e.g.*, *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 620 F. Supp. 2d 1081, 1114 (C.D. Cal. 2008); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d at 1181-82.

party vendor platforms because it “merely provided the forum for an independent third party seller to list and sell his merchandise . . . [and that] Amazon was not actively involved in the listing, bidding, sale or delivery of [the infringing item].”³¹⁹ The court determined that “right and ability to control” must entail more than simply the ability to remove or block access to materials posted on a Web site or stored on a system, because Section 512 specifically requires the service provider to have the ability to takedown or block infringing content.³²⁰

The Ninth Circuit in *UMG Recordings v. Shelter Capital Partners* affirmed the district court’s holding that the “ability to control” has to mean “something more” than the ability to remove infringing material.³²¹ Because the DMCA requires a provider to remove or disable access to material upon having actual and red flag knowledge, the court affirmed the lower court’s ruling that “Congress could not have intended for courts to hold that a service provider loses immunity under the safe harbor provision of the DMCA because it engages in acts that are specifically required by the DMCA.”³²² The circuit court analyzed the statutory language anew without reference to the vicarious liability standard, and concluded that, in this context, the ability to control is item-specific and that to exercise “power or authority” over any particular infringing item, it must be aware of it.³²³ Notably, the court cited to the district court decision in *Viacom* for the principle that “[T]he provider must know of the *particular* case before he can control it.”³²⁴

The Second Circuit in *Viacom International v. YouTube* agreed that the “ability to control” requirement means “something more” than the ability to remove infringing material. First, the court stated that, as a general rule, when Congress uses terms that have accumulated settled meaning under the common law, unless Congress otherwise states, it must be inferred that Congress meant that settled meaning.³²⁵ The court recognized that, under the common law vicarious liability standard, the ability to block an infringers’ access was evidence of the right and ability to su-

³¹⁹ 351 F. Supp. 2d at 1109.

³²⁰ *Id.* at 1110; *see also* *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d at 1153. Similarly, in *Hendrickson v. eBay*, the court ruled that the online auction site’s “voluntary practice of engaging in limited monitoring of its Web site” for infringements “cannot, in and of itself, lead the Court to conclude that eBay has the right and ability to control infringing activity.” 165 F. Supp. 2d at 1094.

³²¹ 667 F.3d 1022, 1041 (9th Cir 2011).

³²² *Id.* at 1042 (citing *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 665 F. Supp. 2d at 1113).

³²³ *Id.* at 1041-42.

³²⁴ *Id.* at 1042.

³²⁵ 676 F.3d 19, 27 (2d Cir. 2012).

pervise or control.³²⁶ Nevertheless, the court rejected Viacom's argument to adopt the common law meaning of the terms, concluding that it "would render the statute internally inconsistent."³²⁷ Section 512(c) presumes that a service provider can block access or remove content, and so, the court reasoned, in order to comply with Section 512(c), a service provider necessarily would have to meet that standard. Thus, the court concluded that while item-specific knowledge is not required, "something more" than the ability to remove or block content is required.

In describing what that "something more" might entail, the Second Circuit in *Viacom* noted two cases in which the service provider was found to have the requisite "right and ability" to control under Section 512. First, it described the findings in *Perfect 10 v. Cybernet Ventures*, the only case to date that has found the service provider had the right and ability to control the infringement under Section 512(c).³²⁸ The defendant in that case had a monitoring program to ensure that users complied with "detailed instructions regard[ing] issues of layout, appearance and content."³²⁹ Access was denied to those who failed to comply. As its second example, the court stated that a defendant liable for *Grokster* inducement might have the required level of control, since inducement infringement "premises liability on purposeful, culpable expression and conduct."³³⁰ This leaves open the possibility of disqualifying YouTube on remand were the court to find YouTube had induced infringement.³³¹

Although it adopted the Ninth Circuit's "something more" standard, the Second Circuit expressly rejected the Ninth Circuit's ruling that a defendant must have item-specific knowledge of an infringing item in order to have the right and ability to control it. It remanded the issue of whether YouTube met this "right and ability to control" standard in Section 512(c)(1)(B) for further fact finding. The Ninth Circuit took note of this in the recent petition for rehearing en banc of *UMG Recordings v. Shelter Capital* and requested supplementary briefing on this issue.³³²

ii) Financial Benefit

Whether the service provider receives a "financial benefit directly attributable to the infringing activity" has received little analysis in the Sec-

³²⁶ *Id.*

³²⁷ *Id.*

³²⁸ 213 F. Supp. 2d 1146, 1173-74 (C.D. Cal. 2002).

³²⁹ *Id.* at 1173 (cited in *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d at 38).

³³⁰ *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d at 38.

³³¹ *Id.*

³³² See Order, *UMG Recordings, Inc. v. Shelter Capital Partners, LLC*, No. 55902 (June 7, 2012), available at http://www.suekayton.com/mbarclay/IPDuckDocs/06-07-12_Order-re-further-briefing.pdf.

tion 512 case law. Despite the fact that this requirement imports language directly from vicarious liability case law, the cases analyzing the financial benefit prong indicate that a heightened standard will be applied in the Section 512 context.

In *CCBill*, the Ninth Circuit acknowledged that “direct financial benefit” under Section 512 should be interpreted consistent with the similarly-worded common law standard for vicarious liability.³³³ The court relied on the legislative history, which states: “receiving a one-time set-up fee and flat, periodic payments for service from a person engaging in infringing activities would not constitute receiving a ‘financial benefit directly attributable to the infringing activity.’”³³⁴ Relying on this, the court concluded that the defendant in *CCBill* did not meet the financial benefit prong of Section 512.³³⁵

In *Capitol Records v. MP3tunes*, the district court held that MP3tunes did not financially benefit from the infringing activity taking place on the site.³³⁶ The court based its decision on legislative history that provided that “a service provider conducting a legitimate business would not be considered to receive a financial benefit directly attributable to the infringing activity where the infringer makes the same kind of payment as non-infringing users.”³³⁷

Some of these Section 512 cases ignore the fact that many service providers today obtain more of a financial benefit from attracting eyeballs, which in turn creates advertising revenue or increased the value of the company, than from subscriber fees or other payments.³³⁸ As a matter of basic statutory interpretation, the courts should look to the vicarious liability case law for guidance here, as well. As described in the discussion of vicarious infringement above, a file hosting service that is directly profiting from or adding value to its site by allowing copyrighted works to be made available on its site should be found to receive a “direct financial benefit”—assuming it can be shown that the infringing content is a draw for users or that infringers pay premium fees.³³⁹

3. *Post-Viacom International v. YouTube and UMG Recordings v. Shelter Capital: The Import of the Recent Section 512 Cases*

As the above discussion reveals, the Ninth and Second Circuits appear to have departed from the common law contributory liability prece-

³³³ *Perfect 10, Inc. v. CCBill, LLC*, 488 F.3d 1102, 1117 (9th Cir. 2007).

³³⁴ *Id.* at 1118 (citing H.R. REP. NO. 105-551, pt. 2, at 54 (1998)).

³³⁵ *Id.*

³³⁶ 821 F. Supp. 2d 627, 645 (S.D.N.Y. 2011).

³³⁷ *Id.*

³³⁸ See *supra* Section I.

³³⁹ See *supra* Section III.2.

dent regarding “knowledge,” where general knowledge that one is enabling mass infringement counts as actual knowledge, regardless of whether the defendant has notice of each and every specific item of infringement. By also interpreting red flag awareness as item-specific and refusing to impose any duty to investigate — even in the face of what, under the common law of contributory infringement, would be constructive knowledge — courts have nearly eviscerated the red flag standard. Based on this interpretation, recent decisions have held that knowledge of pervasive and ubiquitous infringement on a service — even if the service is also facilitating and encouraging the infringement — by itself is never a red flag.

This interpretation of “red flags” as requiring awareness of specific identifiable infringing items is based in large part on the courts’ understanding of Section 512(m), which provides that it is *not* a condition of eligibility for a service provider to “monitor . . . its services or affirmatively seek . . . facts indicating infringing activity.”³⁴⁰ The *Veoh* and *Viacom* courts have held that Section 512(m) means that a service provider should *never* have to conduct any searches, however simple, to remain protected under section 512(c). Section 512(m) does not state this, however. It simply states that investigation is not a necessary “condition” of eligibility. As the legislative history set forth above provides, once a service provider becomes aware of red flags, it must then take action and, in doing so, must further investigate the red flags: “[I]f the service provider becomes aware of a ‘red flag’ from which infringing activity is apparent, it will lose the limitation of liability if it takes no action.”³⁴¹ While Section 512(m) does not impose an obligation to monitor or seek out infringement prior to having red flag knowledge, once a service provider does have red flag awareness that infringement is occurring on its service, it should have an obligation to take simple measures to follow up on those red flags by lo-

³⁴⁰ 17 U.S.C. § 512(m) provides that:

Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on—

(1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i); or

(2) a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law.

See *Viacom Int’l, Inc., v. YouTube, Inc.*, 718 F. Supp. 2d 514, 525 (S.D.N.Y. 2010), *rev’d and remanded in part and aff’d in part*, 676 F.3d 19 (2d Cir. 2012). “General knowledge that infringement is ‘ubiquitous’ does not impose a duty . . . to monitor or search its services for infringement.”

³⁴¹ S. REP. NO. 105-190, at 44 (1998).

cating and removing the instances of obvious infringement.³⁴² Not doing so should be tantamount to willful blindness, as the courts found in the *Cybernet*, *Fung* and *Aimster* cases discussed above. It behooves the courts to consider the Seventh Circuit's reminder that "[t]he common element of the safe harbors is that the service provider must do what it can reasonably be asked to do to prevent the use of its service by repeat infringers."³⁴³ Instead, the Second and Ninth Circuits have placed the burden solely on the right holder, even where it is vastly easier for the service provider to identify and locate the infringing material on its service, e.g., multiple copies of an infringing work identified in a takedown notice or locker copies.

In requiring such a high level of actual and red flag knowledge — such that the precise infringing item and by implication its location need be known — the courts have created a standard that generally only will be met if a DMCA compliant takedown notice is received.³⁴⁴ The import is that a file hosting service that complies with DMCA notices, has a registered DMCA agent and does not control and benefit from the infringement cannot be found liable for encouraging and facilitating infringement on its site generally, but only for any specific items of infringement of which it can be shown it had specific knowledge. Under this interpretation, if Section 512 had been at issue in *Grokster*, for instance, instead of finding inducement for all of the plaintiffs' works that were infringed, a court might find the defendants liable only if and to the extent the plaintiffs could prove that the defendants had knowledge of specific infringing materials. By analogy, if the swap meet operator in *Fonavisa* had been held to this standard, it would have had to name every infringing cassette

³⁴² See JANE C. GINSBURG, *User-Generated Content Sites and Section 512 of the U.S. Copyright Act*, in COPYRIGHT ENFORCEMENT AND THE INTERNET (INFORMATION LAW SERIES) 193 (Irini A. Stanatoudi ed., 2010) ("Section 512(m)'s dispensation of service providers from 'affirmatively seeking facts indicating infringing activity' should not be entitle the service provider to passive-aggressive ignorance.").

³⁴³ *In re Aimster Copyright Litigation*, 334 F.3d 643, 655 (7th Cir. 2003).

³⁴⁴ While most of the courts have not actually stated that compliance with notice and takedown procedures automatically qualifies a provider, the bias in favor of providers that do comply is very strong. See, e.g., *Perfect 10, Inc. v. CCBill, LLC*, 488 F.3d 1102, 1109 (9th Cir. 2007) ("We hold that a service provider 'implements' a policy if it has a working notification system, a procedure of dealing with DMCA-compliant notifications, and if it does not actively prevent copyright owners from collecting information needed to issue such notifications."); *Viacom Int'l, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d at 523 ("Indeed, the present case shows that the DMCA notification regime works efficiently: when Viacom over a period of months accumulated some 100,000 videos and then sent one mass takedown notice on February 2, 2007, by the next business day YouTube had removed virtually all of them.")

tape by title and artist and the booth at which it was sold in order to be found liable.

If the district court in *Viacom v. YouTube* on remand finds specific knowledge, whether actual or red flag, in any of the instances flagged by Viacom, it will have to determine whether YouTube's liability, if any, extends only to those specific instances or whether it will lose the safe harbor for all acts of infringement. Will YouTube only be liable for damages for those instances of infringement where Viacom can prove YouTube had specific knowledge?³⁴⁵ Should this be the result if, as the record appears to show, YouTube knowingly built its business on infringing content? Of course, as the Second Circuit noted, to the extent YouTube is found to have the requisite knowledge of specific works, in order to afford Viacom a remedy, these works must have been alleged to have been infringed in Viacom's complaint.

An important issue is that the Second and Ninth Circuits both rely on the relief provided to rights holders through the notice and takedown procedures and have been reluctant to find knowledge in the absence of a DMCA notice. The Ninth Circuit has essentially stated that the essence of Section 512 is the cooperation induced by the notice and takedown procedures³⁴⁶ and that a copyright holder that does not take advantage of notice and takedown procedures should not later be allowed to bring suit. While the Second Circuit in *Viacom* has held that actual knowledge can come from sources other than a takedown notice (e.g., YouTube's internal knowledge), the Ninth Circuit has expressly limited actual knowledge to knowledge obtained from a takedown notice submitted by the copyright owner. The Second and Ninth Circuits' reliance on notice and takedown process to curtail infringement is misplaced. Congress enacted compliance with the notice and takedown process as an entirely separate provision from the knowledge and awareness requirements, because even then it understood there would be cases where knowledge would be obtained other than through DMCA notices.³⁴⁷ There's no ambiguity in the statute — Congress provided that, in order to take advantage of Section 512, the

³⁴⁵ YouTube had destroyed all of the e-mails from that period under its retention policies, but one of the co-founders who had left YouTube had retained copies of the e-mails on his personal computer. Memorandum of Law in Support of Viacom's Motion for Partial Summary Judgment on Liability and Inapplicability of the Digital Millennium Copyright Act Safe Harbor Defense, *supra* note 168, at 22.

³⁴⁶ 17 U.S.C. § 512(c)(1)(C), (c)(3) (2006).

³⁴⁷ *Id.* Section 512(c)(1)(A) requires removing content promptly upon "actual knowledge" or "awareness of facts and circumstances," whereas 17 U.S.C. § 512(c)(1)(C), requires removing content upon a receipt of a DMCA compliant notice under Section 512(c)(3).

service provider must not have no actual or red flag knowledge, *and* comply with DMCA notices.³⁴⁸

Contrary to what courts seem to believe, notice and takedown procedures are hardly a panacea. No matter how many resources a copyright owner puts into engaging in notice and takedown and how well the service provider complies, as we have seen, it does not appear to be an effective or efficient means of combating infringement. For high-traffic file hosting sites, notice and takedown can only scratch the service of the vast quantities of infringing content, and whatever is taken down is typically put right back up.³⁴⁹ Also, contrary to what some courts have stated, copyright holders are not necessarily in a better position to identify infringing copies of their material on a service and notify the service provider. Although the copyright owner may know what it owns, it is not privy to all copies of a file hosting service. Nor does a copyright owner have the ability to search a third-party file hosting service for its content, much less filter that content — the only reasonably effective way to remove infringing content from many services.

Why did the courts feel the need to create a novel, higher standard of knowledge and awareness for Section 512 that requires item and location specific knowledge and in effect, turns Section 512 into a pure takedown statute? Without a doubt, the case law arose out of valid concerns. Because any site that allows users to post content will very likely be hosting some infringing content, courts understandably do not want to hold a service that innocently does so liable. Plainly, Section 512 was intended to protect such services. Therefore, actual and red flag knowledge have to mean more than purely speculative knowledge — i.e., that there likely is some infringing content somewhere on the service. However, there is a

³⁴⁸ See *Montclair v. Ramsdell*, 107 U.S. 147, 152 (1883) (Harlan, J.) (Court should give effect, if possible, to every clause and word of a statute).

³⁴⁹ *Some Clear Facts About Google's Transparency Report*, RIAA MUSIC NOTES BLOG (May 30, 2012), http://www.riaa.com/blog.php?content_selector=riaa-news-blog&blog_selector=Clear-Facts-&news_month_filter=5&news_year_filter=2012 (“For example, in a recent one month period, we sent Google, and the site in question, multiple DMCA notices concerning over 300 separate unauthorized copies of the same musical recording owned by one of our member companies. Yet that song is still available on that site today . . .”). Moreover, notice and takedown is very costly for the service provider, as well as the copyright owner. Viacom reportedly spends approximately \$100,000 per month to find infringing videos and have them removed from YouTube and other Web sites. See Kevin Delaney, *YouTube Magic: Now You See It, Now You Don't*, WALL ST. J., Aug. 8, 2007, at A1. Small independent artists and distributors obviously don't have the resources to maintain and implement such a full-scale notice and takedown policy, which is ineffective in the long-run to actually keep infringing copies off of unauthorized Web sites.

wide swath of “knowledge” between speculative knowledge and specific knowledge of each and every item of infringing content. As in the contributory liability cases, the courts are capable of distinguishing between the case where a service knows there might be infringing content and where a service knows it is swarming with infringing material, whether or not it can list every single infringing item. With the Section 512(c) red flags standard, Congress was attempting to capture a form of culpable knowledge that lies between such highly general and highly specific knowledge — that is, whether the provider has sufficiently culpable knowledge such that it should be required to take some action.

Part of the problem stems from the diametric manner in which the Second and Ninth Circuits have framed the question of what “actual” and “red flag” knowledge mean. The courts asked whether knowledge means specific knowledge of each individual infringing item or general, speculative knowledge that infringement is occurring on the site.³⁵⁰ Rather than frame the question of a defendant’s knowledge and awareness as either item-specific or general and speculative, courts would better serve the purposes of Section 512 to think in terms of culpable and non-culpable knowledge. This is exactly what the Seventh Circuit did in *Aimster* and the Fourth Circuit did in *ALS Scan v. Remarq*. The courts in those cases understood that Section 512 protection is directed toward the innocent, not those who are aware that their service is being used for massive infringement, encourage it and cannot be bothered to take any action, however simple, to address infringement. As the court in *ALS Scan* stated:

The DMCA’s protection of an innocent service provider disappears at the moment the service provider loses its innocence, i.e., at the moment it becomes aware that a third party is using its system to infringe. At that point, the Act shifts responsibility to the service provider to disable the infringing matter, “preserv[ing] the 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.”³⁵¹

With regard to “right and ability to control” and “economic benefit,” the Second and Ninth Circuits have similarly deviated from the contributory liability common law standards and imposed heightened requirements in the context of Section 512. Those courts have provided that the “right and ability to control” standard in Section 512(c) requires “something

³⁵⁰ *Viacom Int’l, Inc., v. YouTube, Inc.*, 718 F. Supp. 2d 514, 522 (S.D.N.Y. 2010), *rev’d and remanded in part and aff’d in part*, 676 F.3d 19 (2d Cir. 2012) (“The principal question is whether ‘actual knowledge’ and ‘awareness of facts and circumstances from which infringing activity is apparent’ mean a general awareness of widespread infringement or actual or constructive knowledge of specific, identifiable infringements of individual items.”).

³⁵¹ *ALS Scan, Inc. v. RemarQ Communities, Inc.*, 239 F.3d 619, 625 (4th Cir. 2001) (quoting H.R. CONF. REP. NO. 105-796, at 72 (1998)).

more” than the ability to remove or block infringing content, which was deemed to be evidence of the right and ability to control in vicarious liability cases (since the ability to stop infringement is the essence of the ability to control it). In addition, the few cases that have analyzed the economic benefit prong in the context of Section 512 have similarly deviated from vicarious liability case law, by refusing to consider whether the infringing content acts as a draw for users. With respect to both the knowledge requirement and the vicarious liability standard, the courts in these cases thus have taken terms with well-established meanings under secondary liability case law and created new standards that make it much more difficult for a plaintiff to establish liability. As the *Viacom v. YouTube* court itself recognized before adopting the “something more” standard, terms used in statutes should be given their well-settled meanings unless Congress provides otherwise. Nevertheless, the Second Circuit in *Viacom* chose to disregard its own advice and the fact that, if Congress had intended something other than the vicarious liability standard when using the identical language in Section 512, it would have so stated.

It has been argued that Congress must have intended different standards for knowledge and ability to control under Section 512(c) because otherwise the safe harbor would never apply to protect against secondary liability. But, that is indeed the case with respect to vicarious liability. Congress used the vicarious liability standard wholesale in Section 512(c)(1)(B); as such, it must be assumed that it meant the vicarious liability standard — so that if a service provider is vicariously liable, it is indeed disqualified under Section 512(c)(1)(B). It is inconceivable that Congress would have used the identical language from the cases that triggered the enactment of Section 512, e.g., *Netcom*, and not intended to incorporate that standard. With respect to contributory liability, Congress did use a slightly higher standard for knowledge than the existing case law. Where the contributory liability case law considers *actual or constructive knowledge* as an essential element to finding contributory liability, Section 512(c) disqualifies a provider on the basis of *actual or red flag knowledge*. As described above, red flag is a slightly higher standard than constructive knowledge. As such, a service provider could be contributorily liable and yet still protected under Section 512.

IV. CONCLUSION

In recent years, the case law in the Second and Ninth Circuits for both direct and indirect copyright liability has developed in a manner that makes it increasingly difficult for copyright owners to enforce their rights with respect to the vast amount of infringement occurring via file hosting services.

As demonstrated above, many courts have set the “volition” standard for finding direct infringement very high; and in the online context where all actions are automated and software-driven, this arguably creates an unrealistic barrier to copyright owners’ establishing direct liability in such circumstances. The *Netcom* volitional standard was intended to protect truly passive conduits and neutral file hosting services, but has been extended to technologies such as Cablevision’s offsite RS-DVR and even the Hotfile and MP3tunes’ services, which have used their user-stored materials to create commercial destinations for a certain type of content.

The ability to hold a service directly liable for publicly performing copyrighted works online has also been severely curtailed by the potential loophole created by the *Cablevision* decision and its recent progeny, *Aero*. As a result, services capable of transmitting a performance from a unique copy of a work to each user may escape liability — even though both the plain text and legislative history of the Copyright Act support a broad construction covering transmissions by “any device or process” and all further acts by which the performance of a work is transmitted or communicated to the public.

At the same time, establishing secondary liability for file hosting services that offer public access to a vast amount of copyrighted content has become increasingly difficult. In recent file hosting cases, courts in the Ninth and Second Circuits have held that even where infringement was ubiquitous and blatant, the provider was protected from secondary liability by the Section 512(c) safe harbor so long as it complied with notice and takedown. This is a result of the courts extending the protection of Section 512 to activities related to making infringing content available, as well as storage, and their interpreting the Section 512(c) eligibility disqualifiers much more strictly than the identical common law secondary liability standards (making it easy to qualify). These courts created heightened standards for knowledge in the Section 512 context, requiring knowledge of each specific infringing item and sufficient information to locate it and remove it without having to conduct any form of search, including a simple word search. These courts also have created a new standard for “ability to control” that requires more than the ability to remove infringing content and stop infringing activity. Given the blueprint provided by the Second and Ninth Circuits, savvy file host services can flagrantly host infringing content and avoid liability by merely complying with takedown notices.

Also troubling is the practice of analyzing eligibility for the safe harbor first and thereby avoiding having to address whether the provider is secondarily liable, on the grounds that, if the provider is protected, there is no need to reach secondary liability. This ignores the existence of potential limited injunctive relief under Section 512(j) and allows the courts to avoid analysis of culpability, even under theories of inducement liability.

As a result, file hosting services that intentionally encourage and profit from, and possibly even induce, infringement may be cleared of any liability or responsibility for effective cooperation with rights holders, other than responding to takedown notices.

Regardless of whether the service provider is getting rich from hosting from the copyrighted content of others, the Second and Ninth Circuits have made clear that they do not believe the service providers in these cases bear any responsibility for deterring infringement. As the court in *CCBill* stated and courts in several other cases have repeated: Congress placed “the burden of policing copyright infringement . . . squarely on the owners of copyright.”³⁵² A strong sentiment echoes throughout these cases that file host services should bear no responsibility for locating infringement through their services, no matter how blatant and “ubiquitous,” and regardless of how relatively simple it might be for the service to locate and remove much of the infringing content.

Certainly, a service provider should not be held liable for every instance of infringing conduct it fails to deter, nor should it be liable simply because there *could be* infringement on its service. But if a *service provider* in fact knowingly *encourages mass* infringement or otherwise is aware that it is a haven for infringement, common sense tells us that this knowledge should be deemed a red flag. And, as stated in the legislative history and described by Judge Posner in *Aimster*, where there are such obvious red flags of infringement, albeit infringement generally, the service provider should be required to take some simple measures to remove infringing material. Filtering technologies, for instance, would be a simple means of avoiding red flag awareness or willful blindness.

The courts all agree that Section 512 was intended to result in cooperation between rights holders and service providers; the question is what the cooperation should look like. Rights holders believe that cooperation should result in some form of effective enforcement — not perfect, but generally effective to impede infringement; service providers have argued, and the Ninth and Second Circuits have agreed, that the cooperation begins and ends with notice and take-down. If going forward, the courts add a dose of common sense to the mix, as the Supreme Court did in *Grokster* and Judge Posner did in *Aimster*, we might find a workable middle ground. Where “the unlawful objective is unmistakable” as the *Grokster* Court stated, the service provider should be held to task and cooperate in an effective manner or risk liability.³⁵³

As more of these cases make their way through the appellate courts and eventually to the Supreme Court, we will undoubtedly see further de-

³⁵² Perfect 10, Inc. v. CCBill, LLP, 488 F.3d at 1113.

³⁵³ Metro-Goldwyn-Mayer v. Grokster, Ltd., 545 U.S. 913, 940 (2005).

velopment and more consistency in the law. For instance, it is possible that courts will find that service providers that induce infringement are disqualified under Section 512(c)(1)(B) because they have the right and ability to control the infringement and financially benefit from it, as the court in *Viacom* suggested might be the case. Assuming the Supreme Court accepts *certiorari* in one of these cases, it behooves the Court to take a step back from these recent decisions and look at the impact of the strained interpretations of volition, public performance, knowledge, and right and ability to control that have evolved — standards that depart from the long-standing meanings ascribed to these terms in the copyright law and also from common sense. When an entity is responsible for intentionally enabling and profiting from mass-scale infringement, it should have some responsibility to effectively cooperate with rights holders.

Fortunately, many major service providers today understand that it is in their interest to cooperate with content owners and are engaging in discussions or have even agreed to cooperate through measures such as filtering or taking action against repeat infringers, for example through the so-called six-strikes policies AT&T, Cablevision, Comcast, Time Warner Cable and Verizon put into effect this summer.³⁵⁴ As we make our way through this period of transition in copyright law, it behooves us all to remember that we cannot take our creative industries for granted and that our nation's enormous creative output is due in large part to the copyright incentives that have been in place for centuries. Whether one believes in strict or lean copyright laws, it makes little sense for Congress and the courts to refuse to allow copyright holders to enforce even their most basic rights under copyright.

³⁵⁴ Under this agreement, each time a user is found to engage in infringing activity, the user will be sent a notice, and by the fifth or sixth notice the ISPs have agreed to take action such as temporarily reducing connection speeds or requiring the user to review and respond to educational information on copyright. See Jared Newman, *Big Media Goes Easy with 'Six Strikes' Anti-Piracy Measures*, TIME (July 8, 2011), <http://techland.time.com/2011/07/08/six-strikes-anti-piracy-measures> (last visited on June 14, 2012); Eleonora Rosati, *ISPs' Six Strikes Enforcement Plan in Force Next July*, THE 1709 BLOG (March 15, 2012), <http://the1709blog.blogspot.com/2012/03/isps-six-strikes-enforcement-plan-in.html> (last visited on June 14, 2012); see also Mike Masnick, *Organization Overseeing Six Strikes Agreement Between Labels and ISPs Includes Advisory Board to Try to Keep Tech Folks Happy*, TECHDIRT (Apr. 2, 2012), <http://www.techdirt.com/articles/20120402/18015918339/organization-overseeing-six-strikes-agreement-between-labels-isps-includes-advisory-board-to-try-to-keep-tech-folks-happy.shtml>.

PART II

COPYRIGHT CORNER

