

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

VIACOM INT'L INC., ET AL.,
Plaintiffs,

v.

YOUTUBE, INC., ET AL.,
Defendants.

Civil No. 07-CV-2103 (LLS)

ECF Case

THE FOOTBALL ASSOCIATION
PREMIER LEAGUE LIMITED, ET AL., on
behalf of themselves and all others similarly
situated,

Plaintiffs,

v.

YOUTUBE, INC., ET AL.,
Defendants.

ELECTRONICALLY FILED

Civil No. 07-CV-3582 (LLS)

**BRIEF OF *AMICI CURIAE* EBAY INC., FACEBOOK, INC., IAC/INTERACTIVECORP,
AND YAHOO! INC. IN SUPPORT OF DEFENDANTS**

TABLE OF CONTENTS

I. STATEMENT OF INTEREST1

II. INTRODUCTION3

III. ARGUMENT4

 A. By encouraging innovation without fear of potentially crippling liability, the DMCA safe harbors have been a huge success.4

 B. The hosting safe harbor applies not merely to storage, but also to automated processes used to make user-contributed material accessible.7

 C. The actual knowledge and “red flag” awareness exceptions should be interpreted narrowly.....9

 D. Congress gave the control and direct financial benefit provisions in the Section 512(c) safe harbor narrow scope.....12

 1. Control over and operation of a service does not amount to control over specific infringing activity.....13

 2. Generalized financial benefit from the operation of an online service that stores and displays user-contributed content does not amount to a financial benefit “directly attributable to the infringing activity.”15

IV. CONCLUSION.....17

TABLE OF AUTHORITIES

Federal Cases

<i>Corbis Corp. v. Amazon, Inc.</i> 351 F. Supp. 2d 1090 (W.D. Wash. 2004).....	8, 13, 15
<i>Costar Group, Inc. v. Loopnet, Inc.</i> 164 F. Supp. 2d 688 (D. Md. 2001).....	8
<i>Ellison v. Robertson</i> 189 F. Supp. 2d 1051 (C.D. Cal. 2002)	14
<i>Hendrickson v. eBay, Inc.</i> 165 F. Supp. 2d 1082 (C.D. Cal. 2001)	13, 14, 15
<i>Io Group, Inc. v. Veoh Networks, Inc.</i> 586 F. Supp. 2d 1132 (N.D. Cal. 2008).....	8, 14
<i>Perfect 10, Inc. v. CCBill LLC</i> 488 F.3d 1102 (9th Cir. 2007)	12
<i>Perfect 10, Inc. v. CCBill LLC</i> 340 F. Supp. 2d 1077 (C.D. Cal. 2004)	15
<i>Perfect 10, Inc. v. Cybernet Ventures, Inc.</i> 213 F. Supp. 2d 1146 (C.D. Cal. 2002)	15
<i>Playboy Enterp. v. Frena</i> 839 F. Supp. 1552 (M.D. Fla. 1993).....	6
<i>Powerex Corp. v. Reliant Energy Servs., Inc.</i> 551 U.S. 224 (2007).....	10
<i>Religious Tech. Ctr. v. Netcom On-Line Comm. Servs.</i> 907 F. Supp. 1361 (N.D. Cal. 1995).....	6
<i>The Cartoon Network LP, LLP v. CSC Holdings, Inc.</i> 536 F.3d 121 (2d Cir. 2008)	8
<i>Twentieth Century Music Corp. v. Aiken</i> 422 U.S. 151 (1984).....	3
<i>UMG Recordings, Inc. v. Veoh Networks, Inc.</i> 620 F. Supp. 2d 1081 (C.D. Cal. 2008)	8
<i>Zeran v. America Online, Inc.</i> 129 F.3d 327 (4th Cir. 1997)	4, 11, 14, 15

Federal Statutes

17 U.S.C. § 512.....	<i>passim</i>
47 U.S.C. § 230(c)	4, 5, 15

Constitutional Provisions

U.S. CONST. art. I, § 8, cl. 8	3
--------------------------------------	---

Legislative History

H.R. CONF. REP. NO. 105-796 (1998).....	14
H.R. REP. NO. 105-551 (1998).....	<i>passim</i>
S. REP. NO. 105-190 (1998).....	<i>passim</i>

Other Authorities

David Armano, <i>It's the Conversation Economy, Stupid</i> , BUSINESS WEEK, April 9, 2007	4
Lev Grossman, <i>Time's Person of the Year: You</i> , TIME, Dec. 13., 2006.....	4
Rob Walker, <i>The Hidden (in Plain Sight) Persuaders</i> , New York Times Magazine, Dec. 4, 2004.	12
Edward Lee, <i>Warming up to User-Generated Content</i> , 2008 U. ILL. L. REV. 1459 (2008).....	4

I. STATEMENT OF INTEREST

Amici curiae eBay, Inc. (“eBay”), Facebook, Inc. (“Facebook”), IAC/InterActiveCorp (“IAC”), and Yahoo! Inc. (“Yahoo”) (collectively, “*amici*”) are some of the best known online service providers. *Amici* file this brief to provide the Court with the perspective of online service providers who have developed popular and innovative services in reliance on the safe harbor provisions of the Digital Millennium Copyright Act (“DMCA”).

eBay created and currently operates the world’s largest online marketplace, bringing together buyers and sellers at the local, national and global levels. Today, eBay has 90 million active users, engaged in transactions across 50,000 unique categories with the richest and deepest inventory of products ever assembled. Founded in 1995, eBay recognized that the Internet would allow individuals and companies interested in a particular product or service to readily identify and locate each other and thus help allow trading among those individuals and companies. As result, eBay succeeded in establishing a \$60 billion market that benefits consumers and promotes competition. At any given moment, over 200 million listings are available for sale on eBay across a multitude of formats that includes auction-style, fixed price and local listings. eBay is recognized the world over as the place to find a great deal on new, used and vintage items. Throughout its history, eBay has served individual buyers and sellers along with businesses ranging in size from part time sole proprietorships to some of the most recognized household brand names and everything in between. Businesses like eBay, therefore, have an enormous global economic and social impact.

Facebook is among the world’s leading providers of online networking services, and is one of the top five most-trafficked websites of any kind in the world. Facebook’s services were first offered in 2004 as a networking site at Harvard University. Six years later, Facebook provides service in over 70 languages to over 400 million active users worldwide, more than 200 million of whom typically log on to the Facebook website on any given day, and more than 100 million of whom access Facebook through mobile devices. Facebook provides tools for each of its users to create a “Profile Page” on which the user can share content, including real-time status updates, links, photographs, video, and interests, as well as educational and professional

background and contact information. Facebook also enables users to create and join groups dedicated to various topics—such as specific businesses or artists, geography, Internet and technology, music, organizations, sports and recreation, and more—and to share content related to those topics.

IAC is a leading Internet company that owns over 50 established and start-up brands including Ask.com, Citysearch, CollegeHumor, The Daily Beast, Evite, Match.com, Pronto, ServiceMagic, and Vimeo. These brands reach many millions of people worldwide and have been recognized as leaders in their segments. Ask.com was one of the first major Internet search engines and has been recognized for its web search technology and focus on providing answers to user queries; today, Ask.com's network of websites answers questions from 220 million people worldwide. Citysearch, founded in 1996, provides listings and user reviews for businesses in over 75,000 locations in the United States. Vimeo, launched in 2004, provides a unique community for sharing original video content and was named one of *Time* magazine's Top 50 Websites for 2009.

Founded in 1994 by Stanford Ph.D. students David Filo and Jerry Yang, Yahoo! began as a hobby and has evolved into a leading global brand that changed the way people communicate with each other, conduct transactions and access, share, and create information. Today, Yahoo! attracts hundreds of millions of users every month through its innovative technology and engaging content and services, making it one of the most trafficked Internet destinations and a world class online media company. Yahoo!'s vision is to be the center of people's online lives by delivering personally relevant, meaningful Internet experiences. Its offerings to users on Yahoo! properties currently fall into five categories: Integrated Consumer Experiences, Applications (Communications and Communities), Search, Media Products & Solutions, and Mobile. The majority of its offerings are available in more than 30 languages. The company is headquartered in Sunnyvale, California, with a presence in more than 25 countries, provinces, and territories.

All of *amici* regularly host material at the direction of their users, and all of *amici* have copyright policies designed to comply with the safe harbor provisions of the DMCA. Millions of

users every day post material that is made available by *amici* on the Internet in real-time. All of *amici* offer services that depend on the DMCA's safe harbors. Accordingly, *amici* have a strong interest in the proper interpretation of 17 U.S.C. § 512(c), and file this brief in order to assist the Court in that effort.

II. INTRODUCTION

The Copyright Act is intended “[t]o promote the Progress of Science and useful Arts” U.S. CONST. art. I, § 8, cl. 8. “Creative work is to be encouraged and rewarded, but private motivation must ultimately serve the cause of promoting broad public availability of literature, music, and the other arts.” *Twentieth Century Music Corp. v. Aiken*, 422 U.S. 151, 156 (1984). Copyright law “reflects a balance of competing claims upon the public interest,” but its “ultimate aim is . . . to stimulate artistic creativity for the general public good.” *Id.*

The DMCA fits neatly into this scheme of balancing multiple factors in order to promote creativity and the general public good. Enacted in 1998, the DMCA was “designed to facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age.” S. REP. NO. 105-190, at 1-2 (1998). In order to strike a balance between the interests of copyright holders and the need to develop a robust Internet, Congress created “safe harbors” to “preserve[] 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.” *Id.* at 20; H.R. REP. NO. 105-551(II), at 49 (1998). Congress hoped to provide “greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities.” S. REP. NO. 105-190, at 20; H.R. REP. NO. 105-551(II), at 49-50.

Plaintiffs' claims seek to undermine the policy choices made by Congress. Plaintiffs' legal arguments, if accepted, would retard the development of the Internet and electronic commerce, create uncertainty for service providers regarding their legal exposure for alleged infringements, and inhibit the growth and development of user-centric online models that, day after day, make the Internet and the world more democratic. TIME famously named “You” the “Person of the Year,” recognizing that the Internet was “a tool for bringing together the small

contributions of millions of people and making them matter.”¹ Nearly half of Internet users between the ages of 13 and 75 have “created content—blogs, music, photos, videos, and Web sites—for others to view online.” See Edward Lee, *Warming up to User-Generated Content*, 2008 U. ILL. L. REV. 1459, 1500 (2008).² These are some of the sorts of developments Congress sought to promote by including the safe harbors in the DMCA.

Congress enacted the Section 512(c) safe harbor to ensure that “the variety and quality of services on the Internet will continue to expand.” S. REP. NO. 105-190, at 8. Should Plaintiffs’ legal theories be endorsed by the Court, the unprecedented growth that collaborative communities have brought to the Internet would be jeopardized. Fear of liability could discourage many Internet service providers from developing platforms for use by the public at large. This impediment is what Congress sought to avoid when enacting the DMCA’s safe harbor provisions. *Amici* urge the Court to reject Plaintiffs’ interpretation of Section 512(c).

III. ARGUMENT

A. **By encouraging innovation without fear of potentially crippling liability, the DMCA safe harbors have been a huge success.**

Congress enacted the safe harbor provisions in the DMCA in order to ensure that the Internet would continue to be a vibrant source of innovation and creativity. Congress recognized that “without clarification of their liability, service providers may hesitate to make the necessary investment in the expansion of the speed and capacity of the Internet.” S. REP. NO. 105-190, at 8. “[B]y limiting the liability of service providers, the DMCA ensures that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand.” *Id.*³

¹ Lev Grossman, *Time’s Person of the Year: You*, TIME, Dec. 13, 2006, available at <http://www.time.com/time/magazine/article/0,9171,1569514,00.html>.

² See also David Armano, *It’s the Conversation Economy, Stupid*, BUSINESS WEEK, April 9, 2007, available at http://www.businessweek.com/innovate/content/apr2007/id20070409_372598.htm.

³ The DMCA was not the first time Congress recognized the danger of allowing service providers to be held liable for content provided by their users. When Congress enacted the Communications Decency Act in 1996, it included a provision that broadly immunized service providers from tort liability for republishing content provided by their users. See 47 U.S.C. § 230(c). As the Fourth Circuit explained in *Zeran v. America Online, Inc.*: “The amount of

Congress's foresight has been and continues to be amply rewarded. Today, 90 million active users of eBay's services have created the world's largest online marketplace. Yahoo! is one of the most trafficked Internet destinations, attracting hundreds of millions of users every month through its innovative technology and engaging content and services. Facebook's over 400 million users share photos and videos, and interact with organizations large and small, every day. IAC's Ask.com network reaches an audience of over 200 million people worldwide. And while these and other online services are used every day by millions of individuals, their reach further extends to non-profits, businesses of all sizes, and even the government. The White House can be found on Facebook,⁴ posts a stream of pictures to Yahoo!-owned Flickr,⁵ and posts videos to IAC-owned Vimeo;⁶ numerous state and local governments use eBay to sell surplus equipment and supplies to generate revenue for their treasuries.⁷ And each of *amici* has also implemented copyright policies pursuant to the safe harbor provisions of the DMCA.

The ability of *amici* and other online service providers⁸ to provide these services (and future services that have yet even to be thought of) depends on the protections afforded them by the DMCA safe harbors. Internet services today commonly allow millions of users each to contribute to a global conversation. While the vast majority of those contributions are entirely lawful, inevitably some will not be. Without the protections of the safe harbors, the possibility of statutory damages—multiplied by thousands of works—could severely hamper innovation on the Internet, contrary to Congress's intent.

information communicated via interactive computer services is . . . staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems.” 129 F.3d 327, 331 (4th Cir. 1997). Congress's purpose in enacting section 230 was “to avoid any such restrictive effect.” *Id.* By including the safe harbors in the DMCA in 1998, Congress simply addressed these same concerns in the context of copyright law.

⁴ See <http://www.facebook.com/WhiteHouse>.

⁵ See <http://www.flickr.com/photos/whitehouse>.

⁶ See <http://www.vimeo.com/whitehousevideos>.

⁷ See <http://pages.ebay.com/government surplus/index.html>.

⁸ Many of Plaintiffs make use of the protections of DMCA safe harbors when it suits their purposes. See generally http://www.copyright.gov/onlinesp/list/a_agents.html (directory of DMCA Service Provider Agents).

The importance of the DMCA's safe harbors to the continued development of online services cannot be understated. In some cases predating the DMCA, courts directly imposed liability on service providers for the infringing conduct of their users. *See, e.g., Playboy Enterp. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993). While other cases held to the contrary, *see, e.g., Religious Tech. Ctr. v. Netcom On-Line Comm. Servs.*, 907 F. Supp. 1361 (N.D. Cal. 1995), the then-uncertainty in the law is precisely why service providers pressed Congress to include the safe harbors in the DMCA. If Plaintiffs' views are allowed to prevail, many companies undoubtedly would conclude that due to the risk of secondary liability, they must divert resources away from the user-focused collaborative models that today are giving users unprecedented power and choice, and that are currently driving innovation and investment. The threat of ruinous liability would mean that other companies and services might never get off the ground in the first place.

It is a simple technological fact that most individuals and organizations cannot do anything on the Internet without relying on online service providers. When a user sends an email, the user must rely on service providers to connect to the Internet, to process and send the email to its destination, and to store that email until it is read by its recipient. When a user offers an item for sale to the Internet at large, a service provider must host the offer. When a proud parent wants to show friends and family the latest picture or video of a growing child, a service provider needs to provide the infrastructure to hold it and allow people to view it. None of these examples suggests an unlawful enterprise, yet the services that support them each can be used in manners that infringe copyright. If online service providers are denied the protections Congress intended by enacting the safe harbors, each of them will need to reassess carefully current practices (which have been developed over the past decade relying on DMCA safe harbors). In some cases, service providers may possibly question the wisdom of continuing to offer these services, or of developing new services that today we cannot imagine, but that tomorrow may seem integral to our daily lives.

Significantly, the DMCA's safe harbors were not enacted in a vacuum. These safe harbors represent a bargained-for legal regime that was negotiated with copyright owners, online

service providers, and academia at the table. *See* S. REP. NO. 105-190, at 5-7. Senator Hatch supervised three months of negotiation between copyright owners and online service providers. *Id.* at 7. The copyright owners were granted a tremendous boon—the ability to get material expeditiously taken down without resort to judicial action (and even to subpoena the identities of alleged infringers), *see* 17 U.S.C. § 512(c)(1)(C) & (h)—and in exchange hosting services are protected by Section 512(c)’s safe harbor.⁹ Plaintiffs now seek through litigation to obtain that which they were unable to obtain via the legislative process. The positions Plaintiffs take in these cases would undermine a legal framework that was debated and enacted by Congress.

B. The hosting safe harbor applies not merely to storage, but also to automated processes used to make user-contributed material accessible.

Section 512(c) generally immunizes a service provider from monetary relief and all but limited equitable relief for “infringement of copyright by reason of the storage at the direction of a user of material.” 17 U.S.C. § 512(c)(1). Plaintiffs argue that when a service provider’s automated processes perform activities necessary to make content accessible on the Internet, its provision of these tools precludes it from seeking protection under the Section 512(c) safe harbor. But those automated processes are undertaken only because the user has directed the service provider to make the material accessible on the Internet—that is, those processes occur “by reason of the storage at the direction of a user of material.” *Id.*

Far from carving such functions out of the safe harbor, Congress contemplated that qualifying Internet service providers would provide them. For purposes of the Section 512(c) safe harbor, the DMCA defines a service provider as “a provider of online services or network access, or the operator of facilities therefor . . .” 17 U.S.C. § 512(k)(1)(B). “This definition includes, for example, services such as providing Internet access, e-mail, chat room and web page hosting services.” S. REP. NO. 105-190, at 54; H.R. REP. NO. 105-551(II), at 64. Provision of these services necessarily requires more than mere storage, and nothing in the legislative history suggests any intent to limit the hosting safe harbor’s protections to simple storage.

⁹ This distinguishes Section 512(c) cases from those that have been brought against peer-to-peer filesharing services, in which the services do not host the allegedly infringing materials and copyright owners do not have recourse to the extrajudicial options in Section 512(c)(1)(C) & (h).

Indeed, the notice-and-takedown process presumes the service provider is making these materials accessible. *See* 17 U.S.C. § 512(c)(1)(C) (to remain within the safe harbor, a service provider must “remove, or disable access to,” material identified in a proper takedown notice). The intent of the safe harbors and established case law would be undone if mere file formatting and other automated adjustments for purposes of user accessibility precluded a service provider from receiving Section 512(c) protection.

Unsurprisingly, then, courts that have interpreted Section 512(c) have uniformly held that the safe harbor is not limited to mere storage, but also protects automated processes used to make user-contributed material more readily accessible. *See* Memorandum of Law In Support of Defendants’ Motion for Summary Judgment (YouTube Br.) at 28-30 (discussing *Corbis Corp. v. Amazon, Inc.* 351 F. Supp. 2d 1090 (W.D. Wash. 2004); *Costar Group, Inc. v. Loopnet, Inc.*, 164 F. Supp. 2d 688 (D. Md. 2001), *aff’d*, 373 F.3d 544 (4th Cir. 2004); *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132 (N.D. Cal. 2008); and *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 620 F. Supp. 2d 1081 (C.D. Cal. 2008)).

These courts’ analyses are consistent with copyright law in the Second Circuit. In *The Cartoon Network LP, LLP v. CSC Holdings, Inc.*, 536 F.3d 121, 131 (2d Cir. 2008), the court was unequivocal: “In determining who actually ‘makes’ a copy, a significant difference exists between making a request to a human employee, who then volitionally operates the copying system to make the copy, and issuing a command directly to a system, which automatically obeys commands and engages in no volitional conduct.” It is ultimately the user-contributor, not an employee, who selects a file for uploading and who engages the “automated process” that enables the material to be made readily accessible by online service providers.

It was common when the DMCA was enacted,¹⁰ as it is now,¹¹ for service providers to

¹⁰ *See, e.g.*, The Web Standards Project, http://archive.webstandards.org/WSP_release_MAIN.txt (August 10, 1998 statement by an “international coalition of leading Web developers” that “[r]esolving incompatibilities among browsers adds at least 25 percent to the cost of building Web sites”).

¹¹ *See, e.g.*, Wikipedia, *Comparison of web browsers*, http://en.wikipedia.org/wiki/Comparison_of_web_browsers#Image_format_support (chart illustrating compatibility issues for various image formats and web browsers).

need to reformat material in order to make it broadly accessible. Nothing in the legislative history of Section 512(c) suggests that Congress intended to omit from the protections of the DMCA the automated processes made available by service providers to facilitate access to user-supplied content. Consistent with the other decisions that have addressed the issue, the Court should hold that these automated processes fall within the protections of Section 512(c).

C. The actual knowledge and “red flag” awareness exceptions should be interpreted narrowly.

Section 512(c) generally does not shield a service provider that has “actual knowledge that the material or an activity using the material on the system or network is infringing” or that is “aware of facts or circumstances from which infringing activity is apparent.” 17 U.S.C. § 512(c)(A)(i) & (ii). The actual knowledge and “red flag” awareness exceptions to the hosting safe harbor were not intended to swallow the safe harbor whole, but to avoid flagrant misuse of the protections of Section 512(c) by providers hosting pure piracy sites.

Amici here focus on red flag awareness. In discussing identical language in the Section 512(d) safe harbor, the Senate and House committee reports explain,

The important intended objective of this standard is to exclude sophisticated “pirate” directories—which refer Internet users to other selected Internet sites where pirate software, books, movies, and music can be downloaded or transmitted—from the safe harbor.

S. REP. NO. 105-190, at 48; H.R. REP. NO. 105-551(II), at 58. “Absent actual knowledge, awareness of infringement as provided in subsection (d) should typically be imputed to a directory provider only with respect to pirate sites or in similarly obvious and conspicuous circumstances, and not simply because the provider viewed an infringing site during the course of assembling the directory.” S. REP. NO. 105-190, at 49; H.R. REP. NO. 105-551(II), at 58. That is, the knowledge disqualifiers were intended to apply only in the most extreme of situations. Mere generalized awareness of infringement on a site is not enough.

Indeed, as the committee reports explain (again in discussing Internet directories and the knowledge disqualifiers in the Section 512(d) safe harbor that are worded identically to those in the Section 512(c) safe harbor), the existence of “one or more well known photographs of a celebrity at a site devoted to that person” is not a red flag. S. REP. NO. 105-190, at 48; H.R. REP.

NO. 105-551(II), at 57. “The provider could not be expected . . . to determine whether the photograph was still protected by copyright or was in the public domain; if the photograph was still protected by copyright, whether the use was licensed; and if the use was not licensed, whether it was permitted under the fair use doctrine.” S. REP. NO. 105-190, at 48; H.R. REP. NO. 105-551(II), at 57-58.

Moreover, even at the time, Internet directories commonly catalogued thousands upon thousands of sites. *See* S. REP. NO. 105-190, at 49; H.R. REP. NO. 105-551(II), at 58 (“The Yahoo! directory, for example, currently categorizes over 800,000 on-line locations . . .”). Congress thus understood that the situation it was discussing would not be limited to a single site. Instead, it recognized that the providers would observe many sites (though still a mere fraction of the total number of sites they catalogued) that contained one or more well-known photographs. The providers would necessarily be aware, as a statistical matter, that at least some of these sites must contain infringing material, even if they did not know *which* sites contained illegal content. Yet the legislative history shows that Congress did not intend to include this generalized awareness within the scope of Section 512(d)(1)(B). The identically worded red flag awareness exception to the Section 512(c) safe harbor must be construed in the same manner. *Powerex Corp. v. Reliant Energy Servs., Inc.*, 551 U.S. 224, 232 (2007) (“identical words and phrases within the same statute should normally be given the same meaning”).

The difficulties Congress recognized in 1998 have only been amplified with time. While 17% of those in the developed world used the Internet in 1998, by 2007 that percentage had more than tripled to 62%.¹² If service providers lacked the practical ability to determine which of their users’ materials were infringing in 1998, that is all the more true for *amici* and other service providers today. More than half of Facebook’s 400 million users log in on any given day, and the average user creates 70 pieces of content every month. At any given moment, there are more than 200 million listings available for sale on eBay. Hundreds of millions of people make use of Yahoo!’s services every month. IAC-owned Vimeo hosts over 10 million videos at any given

¹² *See* International Telecommunications Union, <http://www.itu.int/ITU-D/ict/statistics/ict/graphs/internet.jpg>.

time and receives an average of 15,000 new video uploads per day. The widespread usage of *amici*'s services, as well as those of other service providers, is the foundation of the democratizing virtues of the Internet, and it would be impossible for service providers to make legal determinations about all of the material they host at the direction of their users. *Cf. Zeran*, 129 F.3d at 333 (“Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context.”). As the House committee explained in its report on an earlier version of the DMCA, the knowledge disqualifiers were intended to make the “criteria for finding contributory infringement . . . somewhat more difficult to satisfy.” H.R. REP. NO. 105-551(I), at 11.¹³ Yet if Plaintiffs’ legal arguments are accepted, service providers would then be subject to a broadened potential secondary liability even where they lack particularized knowledge regarding what material is infringing and should be removed.

The text of the statute confirms that the knowledge disqualifiers require more than generalized awareness of infringement. Even if a service provider has actual knowledge or red flag awareness of infringement, it still does not lose the protection of the hosting safe harbor if “upon obtaining such knowledge or awareness, [it] acts expeditiously to remove, or disable access to, the material.” 17 U.S.C. § 512(c)(1)(A)(iii). If mere generalized awareness of infringement were enough to satisfy Section 512(c)(1)(A)(ii), such a provider¹⁴ would need affirmatively to search for specific infringing material in order to remain within the safe harbor. Section 512, however, expressly provides that the applicability of the safe harbors is not conditioned on “a service provider monitoring its service or affirmatively seeking facts indicating infringing activity” *Id.* § 512(m)(1).

¹³ This Report discussed a version of the safe harbors that differed in several respects from Section 512(c) as enacted, but that prior version of the House bill included language identical to the knowledge disqualifiers in the enacted version of Section 512(c). *See id.* at 8 (proposed Section 512(a)(3)).

¹⁴ It bears noting that the DMCA presupposes that service providers regularly will host infringing material at the direction of users—that is the entire reason why Section 512(c), its notice-and-takedown system, and its grant of immunity exists. Congress cannot have intended that the mere awareness that some users are infringing, without awareness of the specific infringing material, be enough to remove a service provider from the safe harbor.

Indeed, modern trends since the DMCA was enacted in 1998 have, if anything, narrowed the circumstances under which infringement would be “apparent” to a service provider. Today, many companies, including Plaintiff Viacom, use third-party marketing firms to engage in stealth marketing campaigns to promote their content. Viacom engaged dozens of separate third-party marketing agencies working on its behalf to post clips from Viacom television programs and movies to YouTube. *See* YouTube Br. at 39-44. These marketing efforts mean that even posts that look like they do not originate with the copyright owner could in fact be authorized uses.

Viacom’s marketing efforts are not isolated instances. Even in 2004, the New York Times reported that “a growing number of marketers [are now] organizing veritable armies of hired ‘trendsetters’ or ‘influencers’ or ‘street teams’ to execute ‘seeding programs,’ ‘viral marketing,’ ‘guerrilla marketing.’”¹⁵ In many instances, *amici* will be unable to determine whether a user’s material is unauthorized infringement or merely stealth marketing. If changes in marketing tactics mean that it has become more difficult to determine what uses of copyrighted content are or are not authorized, that means that facts sufficient to create red flag awareness are, today, less likely.¹⁶ It does not counsel for a broader interpretation of the knowledge disqualifiers.

Amici respectfully urge the Court to reject Plaintiffs’ attempt to broaden the knowledge disqualifiers of the DMCA’s safe harbors. Plaintiffs’ view of Section 512(c) would slow development of the Internet by making the hosting of user generated content an activity fraught with legal peril. The DMCA was intended to avoid just this result.

D. Congress gave the control and direct financial benefit provisions in the Section 512(c) safe harbor narrow scope.

A service provider is disqualified from protection under the Section 512(c) safe harbor if it “receive[s] a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity.” 17 U.S.C. § 512(c)(1)(B).

¹⁵ Rob Walker, *The Hidden (in Plain Sight) Persuaders*, New York Times Magazine, December 4, 2004, available at <http://www.nytimes.com/2004/12/05/magazine/05BUZZ.html>.

¹⁶ *Cf. Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1114 (9th Cir. 2007) (discussing limits on red flag awareness and concluding, “We do not place the burden of determining whether photographs are actually illegal on a service provider.”).

A service provider loses the safe harbor protection only if the copyright holder can show *both* that the service provider had “the right and ability to control” the infringing activity *and* received “a financial benefit directly attributable to the infringing activity.” *Id.*; *Corbis*, 351 F. Supp. 2d at 1109. If a service provider lacks *either* the practical ability to control infringing activity or the receipt of a financial benefit “directly attributable” to the infringement, it is fully entitled to the protections of the Section 512(c) safe harbor.

1. Control over and operation of a service does not amount to control over specific infringing activity.

In order to qualify for the Section 512(c) safe harbor, a service provider must expeditiously remove or disable access to allegedly infringing material upon receipt of an appropriate notice. 17 U.S.C. § 512(c)(1)(C). The capacities to control and remove material are features that an Internet service provider that stores content must have in order to be eligible for the safe harbor, and thus cannot alone qualify as the “right and ability to control” required by Section 512(c)(1)(B). “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.” *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1093-94 (C.D. Cal. 2001).

Nor would the fact that a provider could implement filtering software to assist in detecting or preventing infringement qualify as the right and ability to control the infringing conduct. Section 512(m) provides that “nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on . . . 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 provision of subsection (i).” If liability were imposed based upon a service provider’s ability to search for potentially infringing files, that would effectively require every service provider to “monitor[] its service or affirmatively seek[] facts indicating infringing activity”—a condition explicitly disclaimed by Section 512(m).

Instead of requiring mere control over the service itself, the statute refers to the right and ability to control “such activity,” referring back to “*the infringing activity.*” 17 U.S.C.

§ 512(c)(1)(B) (emphasis added). By requiring control over “the” infringing activity, the statute focuses on the particular infringing activity at issue, rather than generalized control over the service. Numerous courts have recognized that this is the only reasonable interpretation of the statute, and Plaintiffs’ contrary reading would create a “self-contradictory catch-22 situation that pits 512(c)(1)(B) and 512(c)(1)(C) directly at odds with one another.” *Ellison v. Robertson*, 189 F. Supp. 2d 1051, 1061 (C.D. Cal. 2002), *aff’d in part and rev’d in part on different grounds*, 357 F.3d 1072, 1079 n.10 (9th Cir. 2004).

In *Hendrickson v. eBay, Inc.*, the court rejected the copyright holder’s arguments that eBay had the “right and ability to control” infringing activity because it had removed listings for infringing items in the past. 165 F. Supp. 2d at 1094. The court also held that eBay’s monitoring of its website for apparent infringements did not constitute the “right and ability to control” infringing activity, because “[t]he legislative history shows that Congress did not intend for companies such as eBay to be penalized when they engage in voluntary efforts to combat piracy over the Internet.” *Id.*; *see also* H.R. CONF. REP. NO. 105-796, at 73 (1998) (“Courts should not conclude that the service provider loses eligibility for limitations on liability under section 512 solely because it engaged in a monitoring program.”).

As the court in *Io* explained, “the plain language of Section 512(c) indicates that the pertinent inquiry is not whether [the service provider] has the right and ability to control its *system*, but rather, whether it has the right and ability to control the *infringing activity*.” 586 F. Supp. 2d at 1151. If a service provider’s control over its own system were sufficient to establish the “right and ability to control” the infringing activity, then the protections of Section 512(c) would be meaningless.

Finally, as discussed above, for practical reasons, service providers cannot review each piece of content submitted by the thousands or in some cases millions of users who use their sites. *See* Part III.C, *supra*; *cf. Zeran*, 129 F.3d at 333 (“Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context.”). To require them to do so “would defeat the purpose of the DMCA and render the statute internally inconsistent.” *Hendrickson*, 165 F.

Supp. 2d at 1093; *see also Corbis*, 351 F. Supp. 2d at 1110; *Perfect 10, Inc. v. CCBill LLC*, 340 F. Supp. 2d 1077, 1104 (C.D. Cal. 2004), *aff'd in part and rev'd in part on different grounds*, 488 F.3d 1102 (9th Cir. 2007); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1181-82 (C.D. Cal. 2002).

As the *Zeran* court noted in the context of 47 U.S.C. § 230(c), if service providers could be subject to liability for their publication of material contributed by users, many would follow the “natural incentive” to censor user-contributed content, whether the content in fact was lawful or not. 129 F.3d at 333. This issue is particularly troubling when considering claims of infringement regarding materials that may be fair uses. *See YouTube Br.* at 53-55. Congress understood that in a brief review of user-posted material, a service provider “could not be expected . . . to determine . . . whether [the use] was permitted under the fair use doctrine.” S. REP. NO. 105-190, at 48; H.R. REP. NO. 105-551(II), at 57-58. Imposing potential liability on service providers for every user-contributed piece of content would have a chilling effect on the freedom and communal development of the Internet.

2. Generalized financial benefit from the operation of an online service that stores and displays user-contributed content does not amount to a financial benefit “directly attributable to the infringing activity.”

It is equally imperative to recognize that a service provider with a business model based on attracting web traffic does not receive a “financial benefit directly attributable to the infringing activity” simply because it hosts some infringing content. Congress understood that service providers must be free to adopt business models that could result in revenue that could be related somehow to infringing activity. Absent such freedom, service providers would need to search out all infringement to ensure that no revenues were derived therefrom. This, however, would be directly contrary to the DMCA’s provision stating that applicability of the safe harbors is not conditioned on “a service provider monitoring its service or affirmatively seeking facts indicating infringing activity” 17 U.S.C. § 512(m)(1).

Congress avoided this predicament by ensuring that even if an online service provider has the right and ability to control the specific infringing conduct at issue, it remains entitled to the protections of the Section 512(c) safe harbor unless it receives a financial benefit “directly

attributable to the infringing activity.” 17 U.S.C. § 512(c)(1)(B). As with the “right and ability to control” clause, the statute focuses on “the” infringing activity. A financial benefit that in some way correlates with the infringing activity, but that is no different in kind from the financial benefit that arises from lawful activity, does not place a service provider outside the safe harbor.

The legislative history describes the difference between the types of financial benefit that Congress considered reasonable and those that are potentially problematic:

In determining whether the financial benefit criterion is satisfied, courts should take a common-sense, fact-based approach, not a formalistic one. In general, 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 of the provider’s service. Thus, 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.” Nor is subparagraph (B) intended to cover fees based on the length of the message (per number of bytes, for example) or by connect time. It would however, include any such fees where the value of the service lies in providing access to infringing material.

S. REP. NO. 105-190, at 44-45; H.R. REP. NO. 105-551(II), at 54. Congress distinguished between service providers “conducting a legitimate business” and those whose value “lies in providing access to infringing material.” *Id.* A service provider that charges a fee by “connect time,” for example, will derive additional revenue for all activities that result in users spending more time on the service—including time spent viewing or downloading infringing material. Similarly, a fee that depends on the “number of bytes” consumed by a user will result in additional revenue every time a user views or downloads additional material (i.e. additional bytes), including infringing material. Nonetheless, Congress did not intend that these constitute a financial benefit *directly attributable* to the infringing activity, because the revenue is no different in kind than that which would be derived from non-infringing activity.

As the House committee explained in its report on an earlier version of the DMCA, its goal was to ensure that the “criteria for finding . . . vicarious liability” became “somewhat more difficult to satisfy.” H.R. REP. NO. 105-551(I), at 11.¹⁷ Services whose only value to their users

¹⁷ The House bill being discussed in this report used the same “financial benefit” language as

is to facilitate copyright infringement, or with pricing that is specifically tied to infringement, may receive a “financial benefit directly attributable to the infringing activity.” This is in stark contrast, however, with service providers operating legitimate businesses with revenue models that do not differentiate between infringing and non-infringing uses. *Amici* all provide services that are widely used by law-abiding citizens and businesses—indeed, in many instances their services are used by state and federal government agencies and officials. These types of services are precisely what Congress had in mind when it explained that “a legitimate business” does not lose the protections of the hosting safe harbor when “the same kind” of revenues are associated with both infringing and non-infringing uses. *See* S. REP. NO. 105-190, at 44-45; H.R. REP. NO. 105-551(II), at 54. Reading Section 512(c)’s “financial benefit” language as broadly as Plaintiffs suggest would be inconsistent with Congress’s intent.

IV. CONCLUSION

Congress intended to provide safe harbors for online service providers that would encourage the robust development of the Internet. Plaintiffs’ lawsuits ignore both the express terms of the Section 512(c) safe harbor and Congress’s intent in drafting the DMCA. The Court should follow Congress’s guidance and reject Plaintiffs’ legal theories.

Dated: May 26, 2010

By: /s/ Asim M. Bhansali
Asim M. Bhansali
KEKER & VAN NEST LLP
710 Sansome Street
San Francisco, CA 94111-1704
Telephone: (415) 391-5400
Facsimile: (415) 397-7188
Attorneys for Amici Curiae

Of Counsel:

Michael S. Kwun
Benjamin W. Berkowitz
KEKER & VAN NEST LLP
710 Sansome Street
San Francisco, CA 94111-1704
Telephone: (415) 391-5400
Facsimile: (415) 397-7188

enacted Section 512(c)(1)(B). *See id.* at 8 (proposed Section 512(a)(3)).