Chicago-Kent College of Law

Scholarly Commons @ IIT Chicago-Kent College of Law

All Faculty Scholarship

Faculty Scholarship

January 2009

Decoding the DMCA Safe Harbors

Edward Lee

IIT Chicago-Kent College of Law, elee@kentlaw.iit.edu

Follow this and additional works at: https://scholarship.kentlaw.iit.edu/fac_schol

Part of the [Intellectual Property Law Commons](#), and the [Science and Technology Law Commons](#)

Recommended Citation

Edward Lee, *Decoding the DMCA Safe Harbors*, 32 Colum. J.L. & Arts 233 (2009).

Available at: https://scholarship.kentlaw.iit.edu/fac_schol/351

This Article is brought to you for free and open access by the Faculty Scholarship at Scholarly Commons @ IIT Chicago-Kent College of Law. It has been accepted for inclusion in All Faculty Scholarship by an authorized administrator of Scholarly Commons @ IIT Chicago-Kent College of Law. For more information, please contact jwenger@kentlaw.iit.edu, ebarney@kentlaw.iit.edu.

Decoding the DMCA Safe Harbors

Edward Lee

Columbia Journal of Law & the Arts (draft)
(forthcoming 2009)

DRAFT Jan. 30, 2009

Abstract

The DMCA is a decade old, which, in Internet time, may well be closer to a century. Although the DMCA safe harbors have helped to foster tremendous growth in web applications in our Web 2.0 world, several very basic aspects of the DMCA safe harbors remain uncertain. These uncertainties, along with the relative lack of litigation over the DMCA in the past ten years, have threatened to undermine the whole purpose of the DMCA safe harbors by failing to inform the public and technology companies of what steps they need to undertake to fall within the safe harbors. In several high profile cases against MySpace, YouTube, and other Internet sites, the clarification of the DMCA safe harbors could prove to be just as important to the Internet as their enactment in 1998. This Essay has attempted to clear up two of the biggest uncertainties regarding the DMCA's relationship to vicarious liability, and the so-called "red flags" theory of knowledge on the part of the Internet service provider. Specifically, under a proper interpretation of the DMCA, courts should (i) reject the "loophole" theory that posits that the DMCA safe harbors provide no immunity from vicarious liability at all, and (ii) require a high burden for proving a "red flags" theory by requiring knowledge of facts that show specific and "obvious" or "blatant" infringement. This Essay offers five principles for courts and Congress to consider in applying or amending the DMCA safe harbors in the future. The DMCA safe harbors should be made truly "safe" harbors, in a way that encourages greater investment in and the development of speech technologies on the Internet, all while encouraging copyright holders to share the burden of reducing infringement by utilizing the DMCA notice and take-down procedure.

Decoding the DMCA Safe Harbors

Edward Lee^{*}

A decade has passed since Congress enacted the Digital Millennium Copyright Act of 1998 (DMCA). This landmark legislation was Congress's first (but hopefully not last) attempt to update copyright law to keep pace with the Internet, which, at the time, was a new technology that made copying and disseminating works around the world incredibly easy and on a scale before unimaginable. The DMCA added to copyright law two provisions whose objectives could not be any more different: Title I gives copyright holders *supra*-copyright protection against the circumvention of digital rights management (DRM) on copyrighted works,¹ while Title II establishes four safe harbors for Internet service providers protecting them from monetary liability under copyright law.² Thus, Title I *expanded* copyright liability, whereas Title II *contracted* it.

Today, it is increasingly clear that the safe harbors for ISPs have become the far more important part of the DMCA, particularly given the abandonment of DRM in the music industry.³ Every Internet company in the United States that deals with content of third-party users—meaning companies such as Amazon, AOL, CNN, eBay, Facebook, Google, MySpace, YouTube, and numerous Internet startups that want to become just as big—must adopt and implement a DMCA policy to fall within the safe harbors. Although websites can forego the DMCA safe harbors without violating copyright law, as a practical matter virtually all such commercial websites in the U.S. attempt to follow and fall within the DMCA safe harbors. Indeed, it would be foolish, if not a breach of corporate fiduciary duty, for any such company not to do so.

Despite the widespread importance of the DMCA safe harbors for Internet companies, basic aspects of the DMCA safe harbors still remain unclear. Astonishingly,

^{*} Associate Professor of Law, The Ohio State University Moritz College of Law. Many thanks to Jonathan Band for comments on an earlier draft, and to Martha Chamallas for feedback on some of the ideas herein. While I periodically advise technology companies, this Essay was not funded, modified, or requested by any company during the writing of the Essay.

¹ 17 U.S.C. § 1201 (2000).

² *Id.* § 512.

³ Initially, it looked the opposite, with the anti-circumvention provision garnering the greatest attention among legal commentators. *See, e.g.,* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519 (1999). However, the huge backlash against DRM among consumers—such as encryption on music files instead of the encryptionless MP3 format—and the growing ambivalence among media companies even to use DRM have greatly diminished the significance of the anti-circumvention provision, at least in certain industries. In the music and book industries, for example, many companies such as iTunes, EMI, Universal Music Group, Warner Music Group, Amazon, Random House, Penguin Group, and Simon & Schuster have abandoned DRM on audio files. *See* Edward Lee, *Warming Up to User-Generated Content*, 2008 UNIV. ILL. L.REV. 1459, 1542 & n.405. Apple CEO Steve Jobs led the initiative to get rid of DRM for music files. *See* Steve Jobs, *Thoughts on Music*, APPLE, Feb. 6, 2007, <http://www.apple.com/hotnews/thoughtsonmusic/>. In January 2009, Apple, whose iTunes is the market leader in selling music files, announced the complete abandonment of DRM on music files sold through iTunes. *See* Scott Kirsner, *Apple's iTunes Changes May Show Digital Rights Management's a Loser*, BOSTON GLOBE, Jan. 12, 2009, http://www.boston.com/business/technology/articles/2009/01/12/apples_itunes_changes_may_show_digital_rights_managements_a_loser/.

even the basic question whether the DMCA safe harbors provide any immunity to vicarious liability is still contested. Mark Lemley suggests that it does not—meaning the DMCA may have a “gaping loophole”⁴—although other commentators disagree.⁵ Unfortunately, the courts have yet to squarely decide the issue, although a few cases have begun to touch upon the issue in passing and without the clearest of reasoning.⁶ Another basic issue that remains uncertain is the scope of a website’s duty to remove potentially infringing material beyond the notice-and-takedown procedure specified by the DMCA. Some copyright holders have argued that Internet companies have more expansive duties to patrol their sites under the so-called “red flags” theory based on the presence of other allegedly infringing materials on their sites. The DMCA appears to be ambivalent: it states that websites have no affirmative duty to monitor their services or to “affirmatively seek[] facts indicating infringing activity,”⁷ while it also imposes a duty to take down material if the website has “actual knowledge that the material or activity is infringing” or is “aware of facts or circumstances from which infringing activity is apparent.”⁸ How these countervailing provisions play out in particular facts has been the source of much contention.

This Essay attempts to clear up some of the major confusion over the DMCA safe harbors. Part I attempts to put to rest the “loophole” reading of the DMCA and explains why the DMCA safe harbors do provide *qualified or partial immunity* to vicarious liability (and all other forms of copyright liability as well). The fundamental flaw of the “loophole” reading is that it mistakenly treats one of the requirements in the DMCA safe harbor as *exactly* the same as the standard of vicarious liability, even though the language in the DMCA is slightly different from—and more restrictive than—the test for vicarious liability. Part II then analyzes the so-called “red flags” theory and the vexing question of when an ISP can be said to be “aware of facts or circumstances from which infringing activity is apparent,” thus giving rise to a duty of take down. Only a few courts have addressed this issue, but all have rejected the arguments of copyright holders to adopt a low standard of proving such awareness of infringement. Agreeing with these decisions, this Essay argues for the adoption of a high standard of proof of specific knowledge of “blatant” or “obvious” infringement. Part III offers future guidance and principles for both courts and Congress to help address the pressing need to clarify and update the DMCA safe harbors as the Internet continues to rapidly evolve.

⁴ Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. TELECOMM. & HIGH TECH L. 101, 104 & n. 23, 113-14 (2007). See also Rebecca Giblin, *A Big Liable? A Guide to Navigating the U.S. Secondary Liability Patchwork*, 25 SANTA CLARA COMP. & HIGH TECH. L.J. 7, 44 (2008) (“DMCA safe harbors provide no protection for vicarious infringement”).

⁵ See Jonathan Band, *Safe Harbors Against the Liability Hurricane: The Communications Decency Act and the Digital Millennium Copyright Act*, 20 CARDOZO ARTS & ENT. L.J. 295 (2002) (“Treating these tests as the same is extremely dangerous because it invites future courts to apply *Napster*’s stringent vicarious liability standards in the DMCA context.”); Charles S. Wright, *Actual Versus Legal Control: Reading Vicarious Liability for Copyright Infringement into the Digital Millennium Copyright Act of 1998*, 75 WASH. L. REV. 1005, 1026-28 (2000); Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833, 1883 (2000).

⁶ See *infra* notes 19-34 and accompanying text.

⁷ 17 U.S.C. § 512(m).

⁸ *Id.* § 512(d)(1).

I. Do the DMCA Safe Harbors Protect Against Vicarious Liability?

Some ten years after the DMCA was passed, it is hard to believe there is still debate over whether it provides any immunity to Internet companies from vicarious liability. By all indications from the legislative history, Congress thought it did. As both the House and Senate reports state unequivocally: “The limitations in subsections (a) through (d) protect qualifying service providers from liability for *all monetary relief* for *all* direct, *vicarious* and contributory infringement.”⁹ However, some commentators have suggested that the DMCA has a huge loophole that carves out vicarious liability from the safe harbors entirely, thereby exposing Internet companies to potentially limitless liability for claims of vicarious infringement. As this Part explains, the “loophole” theory is wrong. The DMCA provides immunity to Internet companies from claims of vicarious infringement, as well as direct and contributory infringement claims. The DMCA safe harbors are not secretly *unsafe* harbors.

A. Relevant Text of DMCA Safe Harbors

Section 512 of the Copyright Act contains the DMCA safe harbors. Four basic safe harbors are set forth in subsections (a) through (d); these provisions immunize Internet service providers from monetary damages by reason of four different kinds of conduct: (a) providing Internet access, (b) system caching or temporary storage of material, (c) passive storage or hosting of material posted by users, and (d) providing location tools, such as links to content on other sites.¹⁰ (There is also a fifth safe harbor limited or tailored to higher education institutions.¹¹) The safe harbors protect only certain *activities* or functions of Internet service providers—something the DMCA itself makes clear in section (n).¹² A single website or Internet company can qualify under all four safe harbors if it engages in all four activities specified in § 512.

The question of potential vicarious liability has arisen in the context of the safe harbors in subsections (c) and (d). Section 512(c)(1)(B) provides the safe harbor for Internet service providers for hosting or storing material posted by their users:

(c) Information residing on systems or networks at direction of users.--

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

⁹ S. Rep. 105-190, at 40 (1998) (emphasis added); H.R. Rep. No. 105-551, pt. 2, at 50 (1998) (emphasis added).

¹⁰ See 17 U.S.C. § 512(a), (b), (c), (d). Subsection (g) also provides immunity under specified conditions for the Internet service provider’s removal of allegedly infringing material pursuant to a DMCA notice from the copyright holder. *Id.* § 512(g).

¹¹ *Id.* § 512(e).

¹² See *id.* § 512(n) (“Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section.”); S. Rep. 105-190, at 40 (1998) (“New section 512 contains limitations on service providers’ liability for five general categories of activity set forth in subsections (a) through (d) and subsection (f)”). In this regard, I think Lemley’s characterization of the DMCA safe harbors as protecting “classes of intermediaries” is not exactly right. See Lemley, *supra* note [], at 104 (DMCA protects “only four classes of intermediaries”).

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—

(A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;

(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(B) *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*; and

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

The same language that is italicized above can be found also in § 512(d)(2), which sets forth the requirements for the safe harbor for activity involving location tools.¹³ Thus, a prerequisite for both the storage and location tool safe harbors is that the ISP “*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.*”

B. Decoding the “Loophole” Theory of the DMCA Safe Harbors

1. The “Loophole” Reading

The above italicized language is the sole basis for the “loophole” theory, and the confusion over whether the DMCA safe harbors, albeit inadvertently, left open a “gaping loophole” by which many Internet companies can potentially be subject to millions of dollars in copyright liability for vicarious infringement.¹⁴ The putative loophole exists because Internet companies cannot fall within the DMCA safe harbors if they “*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,*” which some commentators have equated as the exact same standard as vicarious liability. If correct, the loophole interpretation of the DMCA may, as Lemley recognizes, “undo the benefits of the safe harbors altogether,” given how easy it is to allege vicarious infringement against Internet companies under the case law.¹⁵

¹³ 17 U.S.C. § 512(d)(2).

¹⁴ Lemley, *supra* note 4, at 114.

¹⁵ *Id.* The Goldstein copyright treatise appears to provide some support for Lemley’s view, although the reference in the Goldstein treatise is very brief and does not explicitly go as far as Lemley’s assertion. *See* 2 PAUL GOLDSTEIN, GOLDSTEIN ON COPYRIGHT § 8.3.2, at 8:42 (3d ed. 2007) (“The second condition for this safe harbor effectively embodies the rules on vicarious liability, and requires that the service

Although Lemley recently suggested the loophole theory, it is unclear whether he himself thinks it is the correct interpretation of the DMCA. Lemley's essay, which focused on a different topic,¹⁶ contains only two sentences floating the theory.¹⁷ The actual support for his theory is contained in footnote 23, which is worth quoting in full:

Id. § 512(c)(1)(B) (safe harbor available only to an intermediary that “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”). The language suggests that it provides a safe harbor under section 512(c) only against claims of direct and contributory infringement, rather than vicarious liability. The legislative history suggests the opposite. See H.R. Rep. No. 105-551, pt. 2, at 50 (1998)(suggesting—wrongly—that the bill would “protect qualifying service providers from liability for all monetary relief for direct, vicarious, and contributory infringement”). And the fact that the statute doesn't use the term vicarious infringement, but instead sets out what were commonly understood in 1998 to be the elements of a vicarious infringement claim, raises additional questions. The Ninth Circuit has steadily whittled away the requirement of “direct financial benefit” as a requirement for vicarious infringement, for instance, to the point where it has held parties liable in the absence of any financial benefit at all, direct or indirect. See *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001); cf. *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259 (9th Cir. 1996) (beginning the whittling away of the “direct financial benefit” requirement completed in *Napster*). And the Supreme Court has created a new tort for inducement of copyright infringement, though it claimed that this new tort was an offshoot of contributory infringement. *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005). Are these new or broadened torts also outside the safe harbor? A plain reading of the statute would suggest not, but to date there is no case law on the issue.¹⁸

Though Lemley may be equivocal on his view of the correct interpretation, I use his essay as a springboard for examining the “loophole” theory because I believe Lemley encapsulates well the theory.

2. *Relevant case law*

Courts have yet to tease out the relationship between vicarious liability and the DMCA safe harbors. Although several courts have discussed different aspects of the issue, the courts have yet to fully explain the precise relationship—I think, in part,

provider “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.”). The Nimmer treatise, however, takes a contrary view and suggests that the DMCA safe harbor only excludes from immunity a more limited set of vicarious liability cases instead of the more expansive, common-law views of vicarious liability in which courts effectively stretched the requirement of “direct financial benefit” to include indirect benefits as well. See 3 MELVILLE B. NIMMER & DAVID NIMMER, *NIMMER ON COPYRIGHT* § 12B.04[A][2][b], at 12B-55 – 12B-56 (2008).

¹⁶ Lemley's essay was meant to provide a panoramic view of several different safe harbors, including the DMCA, and to offer a single, common approach to Internet safe harbors. Lemley, *supra* note 4, at 101-02. Unfortunately, I do not have the space here to discuss the merits of Lemley's very interesting proposal. I focus instead on his suggestion that the DMCA safe harbors do not work against vicarious liability, but I do not want to make more out of Lemley's suggestion than he intended.

¹⁷ *Id.* at 104, 114-15.

¹⁸ *Id.* at 104 n.23.

because the DMCA itself is not a model of clarity. The Fourth and Ninth Circuits have produced the most relevant case law; each is discussed in turn.

a. Fourth Circuit

The Fourth Circuit’s case law cuts against the loophole interpretation. In dictum, the district court in *Costar* appeared to adopt something close to the loophole position, stating that “[b]asically, the DMCA provides no safe harbor for vicarious infringement because it codifies both elements of vicarious liability.”¹⁹ We should not read too much into this statement, however. The dictum was qualified by the district court’s own analysis, which required a fairly strict showing that defendant received a financial benefit “directly attributable to the infringing activity.”²⁰ That strict standard was not satisfied where the users of defendant’s real estate website made no payments of any kind to the defendant.²¹ The district court even rejected the argument that “enhanc[ing] the attractiveness of the venue to potential customers”—something that could easily be considered a financial benefit under vicarious liability case law—constituted the kind of disqualifying financial benefit that fell outside the DMCA.²² In the court’s view, such a benefit was only an indirect benefit.²³

The Nimmer treatise believes the district court’s opinion in *Costar* correctly applied a stricter standard for “*a financial benefit directly attributable to the infringing activity*” than courts have applied rather loosely in vicarious liability cases for the direct financial benefit prong. According to the Nimmer treatise:

In the context of this safe harbor, Judge Chasanow in *Costar Group Inc. v. LoopNet, Inc* took the requirement of “direct financial benefit” literally. That construction stands in contrast to the gloss on “direct financial benefit,” an element of vicarious liability as defined at common law—in which courts are so non-literal as to be willing to construe past judicial references to “direct” as meaning, essentially, “indirect.” But whereas those courts were spinning out interpretation of a common law standard, and thereby enjoyed the authority to construct new interpretation consonant with their sense of justice, presumably much less latitude applies to the task of construing the language that Congress employed in a statute.²⁴

However one reads the district court’s opinion, the court’s dictum suggesting that vicarious liability falls outside the DMCA safe harbor was later *rejected* by the Fourth Circuit, which held that the DMCA safe harbors apply to both vicarious and contributory infringement:

¹⁹ *Costar Group Inc., v. LoopNet, Inc.*, 164 F. Supp. 2d 688, 704 (D. Md. 2001), *aff’d*, 373 F.3d 544 (4th Cir. 2004).

²⁰ *Id.* at 705.

²¹ *Id.*

²² *Id.*

²³ *Id.*

²⁴ See 3 NIMMER & NIMMER, *supra* note 15, at 12B-55 – 12B-56.

An ISP, however, can become liable indirectly upon a showing of additional involvement sufficient to establish a contributory or *vicarious violation of the Act*. In that case, the ISP could still look to the DMCA for a safe harbor if it fulfilled the conditions therein.²⁵

Although the court did not discuss the relationship between the DMCA and vicarious liability at length, it did characterize § 512(c)(1)(B) as requiring that the defendant “does not profit directly from the violation”²⁶—an interpretation that is close to the one I advance later in this Essay.

b. Ninth Circuit

The Ninth Circuit’s case law is a little bit more mixed. Giving some support to the “loophole” reading, the case law does suggest that the DMCA codifies the same standard of “direct financial benefit” as the common law standard for vicarious liability. As the Ninth Circuit explained in *Perfect 10, Inc. v. CCBill LLC*:

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 these terms,” *Rossi*, 391 F.3d at 1004 n. 4 (9th Cir. 2004) (quoting *Neder v. United States*, 527 U.S. 1, 21, 119 S. Ct. 1827, 144 L.Ed.2d 35 (1999)), we hold that “direct financial benefit” should be interpreted consistent with the similarly-worded common law standard for vicarious copyright liability. *See, e.g., Ellison*, 357 F.3d at 1078 (a vicariously liable copyright infringer “derive[s] a direct financial benefit from the infringement and ha[s] the right and ability to supervise the infringing activity”). Thus, the relevant inquiry is “whether the infringing activity constitutes a draw for subscribers, not just an added benefit.” *Id.* at 1079. In *Ellison*, the court held that “no jury could reasonably conclude that AOL received a direct financial benefit from providing access to the infringing material” because “[t]he record lacks evidence that AOL attracted or retained subscriptions because of the infringement or lost subscriptions because of AOL’s eventual obstruction of the infringement.” *Id.*²⁷

Yet, in practice, the Ninth Circuit appears to have applied the DMCA safe harbor in a way to require a fairly high level of proof for direct financial benefit, perhaps higher than the common law standard. In *CCBill*, the Ninth Circuit went on to rely on the examples in the legislative history that “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.’”²⁸

It is difficult to discern how far the Ninth Circuit meant to go in holding that “‘direct financial benefit’ should be interpreted consistent with the similarly-worded common law standard for vicarious copyright liability.”²⁹ For various reasons, I do not believe we can take it as an endorsement of the “loophole” reading of the DMCA.

²⁵ CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544, 555 (4th Cir. 2004).

²⁶ *Id.* at 552.

²⁷ *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1117-18 (9th Cir. 2007).

²⁸ *Id.* at 1118 (quoting H.R. Rep. 105-551 (II), at 54 (1998)) (emphasis added).

²⁹ *Id.* at 1117.

First of all, the court never went as far as to hold that all vicarious liability claims fall outside of the DMCA safe harbor. As I discuss later below, most courts have interpreted another part of the DMCA safe harbor—i.e., the “*right and ability to control such activity*”—in a way that is more narrow than the analogous standard under vicarious liability.³⁰

Second, as the *CCBill* case suggests, the Ninth Circuit’s more recent case law may be tightening the requirements of proof for vicarious liability compared to the looser “direct financial interest” approach of the common law, in order to match it with the stricter standard of the DMCA. In essence, the DMCA standard might be having a reverse effect on vicarious liability law, effectively tightening the requirements of proof there. For example, *Ellison v. Robertson*,³¹ the case cited in *CCBill*, applied a fairly strict standard of “direct financial benefit” under vicarious liability. The case involved the unauthorized postings of Harlan Ellison’s works by a third party onto a USENET news group accessible on AOL to its users (who paid for AOL service).³² The court held that the plaintiff failed to establish a triable vicarious infringement claim against AOL because there was no evidence to establish a causal connection “between AOL’s profits from subscriptions and the infringing activity taking place on its USENET servers.”³³ The court found no evidence that “AOL attracted or retained [paid] subscriptions because of infringement.”³⁴

In short, the cases from the Ninth Circuit are still evolving. None has squarely decided whether the DMCA safe harbors provide no immunity from any vicarious liability claim.

C. Why the “Loophole” Theory Is Wrong

The “loophole” theory of the DMCA safe harbor rests on the similarity in language between the DMCA’s requirement that the ISP “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,” and the requirements of vicarious liability. This similarity, however, is too slender a reed on which to base a “gaping loophole” to the DMCA.

1. *The text of the DMCA is not exactly the same as traditional vicarious liability standards*

First things first: the text. The plain language of the DMCA is *not* the same as the standard of vicarious liability. The loophole interpretation erroneously concludes that the language in the DMCA safe harbor—“*does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right*

³⁰ See *infra* notes 63-69 and accompanying text.

³¹ 357 F.3d 1072 (9th Cir. 2004).

³² *Id.* at 1074.

³³ *Id.* at 1079.

³⁴ *Id.*

and ability to control such activity”—is the same as the language for the traditional standard of vicarious liability.³⁵ Not so.

Indeed, no court has ever used the exact same language of the DMCA to describe the standard of vicarious liability under copyright law. Although similar, the traditional standard of vicarious liability is that secondary liability will attach “if [the defendant] has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities.”³⁶

True, the requirement regarding the defendant’s “right and ability” to control or supervise the infringing activity appears to be very similar to, if not the same as, the DMCA wording. But the words of the DMCA’s “financial” requirement are different than the copyright standard of vicarious liability and appear to be stricter. In the DMCA, the defendant must “*not receive a financial benefit directly attributable to the infringing activity.*” By contrast, under the traditional standard for vicarious liability, the defendant must not have “a direct financial interest in such activities,”³⁷ or, in other cases, obtain a “direct financial benefit from the infringement.”³⁸

Although similar to the common law standard, the DMCA wording is *not* the same. Indeed, the phrasing in the DMCA—“receive a financial benefit directly attributable to the infringing activity”—has *never* been used before by any federal court to describe the standard for vicarious liability. Nor has it ever been used by any state court in any case in any area of law. The phrasing is Congress’s own creation.

There are at least two key differences in Congress’s wording. First, the DMCA speaks of “receive” a financial “benefit.” That appears to require something more than just “having” a financial “interest,” the standard mentioned in some of the seminal vicarious liability classes. For example, I might own 100,000 shares in a startup company that has yet to begin its business, has earned no revenue at all, and whose shares are nontransferable and worth virtually nothing. Clearly, I “have” a financial “interest” in the startup company, but, under the ordinary meaning of the terms, I would be hard pressed to say that I have actually “received” a financial “benefit” yet from shares that are worth nothing.

³⁵ This same mistake is made even by some commentators who argue against the “loophole” reading. *See, e.g., Wright, supra* note 5, at 1007 (“This language tracks the test for vicarious liability for copyright infringement. Because a vicariously liable service provider by definition has control and receives a direct financial benefit, the plain language of this bar makes the safe harbor unavailable to any service provider that has already been found vicariously liable.”).

³⁶ *Gershwin Publ’g Corp. v. Columbia Arts Mgmt., Inc.*, 443 F.2d 1159, 1162 (1971); *see also* *Shapiro, Bernstein Co. v. H.L. Green Co.*, 316 F.2d 304 (2d Cir. 1963) (same); *CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544, 550 (4th Cir. 2004); *Gordon v. Nextel Commcns. & Mullen Advertising*, 345 F.3d 922, 925 (6th Cir. 2003); *Hard Rock Café Licensing Corp. v. Concession Servs., Inc.*, 955 F.2d 1143, 1150 (7th Cir. 1992) (same); *RCA/Ariola Int’l, Inc. v. Thomas & Grayston Co.*, 845 F.2d 773, 781 (8th Cir. 1988) (same); *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1022 (9th Cir. 2001) (same).

³⁷ *See, e.g., Gershwin*, 443 F.2d at 1162; *Costar*, 373 F.3d at 550.

³⁸ *See, e.g., Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 262 (9th Cir. 1996).

The second key difference is that the DMCA has the language “*directly attributable* to infringing activity,” a locution that no case in copyright law has ever used to describe vicarious liability. Although similar to the vicarious liability standard, the phrasing chosen by Congress is different and appears to require a greater level of attribution or causation. The financial benefit must be “directly attributable” to the infringing activity.

Given the difference in wording between the DMCA’s requirement of “*a financial benefit directly attributable to the infringing activity*” and the common law vicarious liability standard of “a direct financial interest (or benefit) in such activities,” the canon of construction that presumes Congress intends to incorporate “the accumulated settled meaning under the common law” simply does not apply.³⁹ That was one of the mistakes of the Ninth Circuit in the *CCBill* case.⁴⁰ In copyright law’s treatment of vicarious liability, no meaning, settled or otherwise, even exists for the term “financial benefit directly attributable to the infringing activity.” That term of art exists only in the statute, *not* in the common law. Under Supreme Court precedents, the canon of common law meaning applies only to statutory terms that are identical with the common law.⁴¹ However, mere similarity to a common-law doctrine is not a basis for applying the canon, particularly where, as here, the statutory terms are worded differently than the common law.⁴²

³⁹ Neder v. U.S., 527 U.S. 1, 21 (1999) (“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 these terms”).

⁴⁰ See Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1117 (9th Cir. 2007).

⁴¹ See, e.g., *id.* at 23-24 (interpreting “defraud” in federal mail fraud, wire fraud, and bank fraud statutes); *Nationwide Mut. Ins. Co. v. Darden*, 503 U.S. 318, 322 (1992) (interpreting “employee” in ERISA); *Evans v. U.S.*, 504 U.S. 255, 261-64 (1992) (interpreting “extortion” in 18 U.S.C. § 1951); *Community for Creative Non-Violence v. Reid*, 490 U.S. 730, 739-40 (1989) (interpreting “employee” and “scope of employment” in Copyright Act); *Standard Oil Co. v. U.S.*, 221 U.S. 1, 59 (1911) (interpreting “restraint of trade” under Antitrust Act).

⁴² See *Carter v. U.S.*, 530 U.S. 255, 264 (2000) (“While we (and the Government) agree that the statutory crimes at issue here bear a close resemblance to the common-law crimes of robbery and larceny, that observation is beside the point. The canon on imputing common-law meaning applies only when Congress makes use of a statutory *term* with established meaning at common law....”) (internal citations omitted); *id.* at 265 (a “cluster of ideas” from the common law should be imported into statutory text only when Congress employs a common-law *term*, and not when, as here, Congress simply describes an offense analogous to a common-law crime without using common-law terms); *Morissette v. U.S.*, 342 U.S. 246, 263 (1952) (“[W]here Congress borrows *terms* of art in which are accumulated the legal tradition and meaning of centuries of practice, it presumably knows and adopts the cluster of ideas that were attached to each borrowed *word* in the body of learning from which it was taken and the meaning its use will convey to the judicial mind unless otherwise instructed. In such case, absence of contrary direction may be taken as satisfaction with widely accepted definitions, not as a departure from them.”) (emphasis added).

In a number of cases, the Supreme Court has interpreted statutory terms, though similar to common law concepts, as different from the common law. See, e.g., *U.S. v. Wells*, 519 U.S. 482, 492 n.10 (1997) (interpreting federal statute, 18 U.S.C. § 1014, making it a crime to knowingly make “false statement” to FDIC insured bank so as not to require proof of materiality required in common law crimes involving false statements such as perjury); *Perrin v. U.S.*, 444 U.S. 37, 43-46 (1979) (Travel Act prohibition against travel or use of facility in interstate commerce to commit “bribery” in violation of state laws had more expansive notion of bribery than common law); *U.S. v. Turley*, 352 U.S. 407, 411-12 (1957) (refusing to apply common law canon to “stolen” in National Motor Vehicle Theft Act so as to limit

2. *Congress knew how to expressly exclude vicarious liability in the DMCA, but chose not to in the DMCA safe harbors*

The structure of the DMCA safe harbors also militates against the “loophole” reading. If Congress’s intent were to carve out vicarious liability from the DMCA safe harbors, it could have simply stated that “Nothing in this section diminishes or immunizes claims of vicarious liability against Internet service providers.” Period, end of debate.

Indeed, in the very same statute dealing with the DMCA anti-circumvention provision (Title I of the Act), Congress did exactly that for an unrelated section dealing with the anti-circumvention provision, which clearly states: “*Nothing in this section shall enlarge or diminish vicarious or contributory liability* for copyright infringement in connection with any technology, product, service, device, component, or part thereof.”⁴³

For the DMCA safe harbors, however, Congress did not include any such provision exempting vicarious liability. One could argue that Congress meant to do the same thing through the words “*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.*” But that suggestion would mean that Congress chose to include an express exclusion of vicarious liability in Title I of the DMCA, but then a different, more convoluted and roundabout exclusion of vicarious liability in Title II of the DMCA.

Such a proposition is unconvincing. As the Supreme Court has recognized, it is doubtful that Congress would adopt an indirect, convoluted wording to achieve the same result as what Congress has achieved expressly by clear wording in a statute,⁴⁴ especially where, as here, it is the very same statute containing the provisions in question, all enacted at the very same time.⁴⁵ There is no explanation for why Congress would

it to common law larceny because “stolen” “has no accepted common-law meaning” and is not a “word of art”).

⁴³ 17 U.S.C. § 1201(c)(2) (emphasis added).

⁴⁴ See, e.g., *Central Bank of Denver, N.A. v. First Interstate Bank*, 511 U.S. 164 (1994) (“[w]hen Congress wished to create such [secondary] liability, it had little trouble doing so”); *Howard Delivery Serv., Inc. v. Zurich American Ins.*, 547 U.S. 651, 676 (2006) (Kennedy, J., dissenting) (“Congress wanted a particular provision of the Bankruptcy Code to narrow the ordinary definition to exclude mandatory workers’ compensation, it did so expressly by referring to those plans covered by ERISA”); *United States v. Smith*, 499 U.S. 160, 172 (1991) (“When Congress wanted to limit the scope of immunity available under the Liability Reform Act, it did so expressly, as it did in preserving employee liability for *Bivens* actions and for actions brought under a federal statute authorizing recovery against the individual employee.”); *Mackey v. Lanier Collection Agency & Serv., Inc.*, 486 U.S. 825, 836 (1988) (“Where Congress intended in ERISA to preclude a particular method of state-law enforcement of judgments, or extend anti-alienation protection to a particular type of ERISA plan, it did so expressly in the statute.”); see also *United States v. McGoff*, 831 F.2d 1071, 1093 (D.C. Cir. 1987) (“we doubt that Congress would choose to exercise such an unusual power implicitly, in such a roundabout fashion, and for an offense which does not partake of the nature of *mala in se*. After all, on the one occasion Congress actually intended to eliminate a statute of limitations, it did so explicitly.”);

⁴⁵ See, e.g., *Offshore Logistics, Inc. v. Tallentire*, 477 U.S. 207, 222 (1986) (“Section 4 indicates that when Congress wanted to preserve the right to recover under the law of another sovereign for whatever measure of damages that law might provide, regardless of any inconsistency with the measure of damages

expressly exclude vicarious liability in the anti-circumvention provision of the DMCA (Title I of the Act), but then adopt a much more convoluted, roundabout way of doing the exact same thing in the DMCA safe harbors (Title II of the Act). Lemley does appear to find it puzzling why Congress would not just refer to vicarious infringement by name in the DMCA safe harbors; as Lemley concedes, “the fact that the statute doesn’t use the term vicarious infringement, but instead sets out what were commonly understood in 1998 to be the elements of a vicarious infringement claim, raises additional questions.”⁴⁶

3. *The DMCA’s purpose and legislative history refute the loophole theory*

Both the Senate and the House Reports indicate that Congress wanted to provide a safe harbor from *all* monetary relief under copyright law, whatever the cause of action. The Reports state:

The limitations in subsections (a) through (d) protect qualifying service providers from liability for all monetary relief for *all* direct, *vicarious* and contributory infringement.⁴⁷

And specifically with respect to the safe harbor in subsection (c) for storage of material, the Reports state:

Subsection (c) limits liability of qualifying service providers for claims of direct, *vicarious* and contributory *infringement* for 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.⁴⁸

Moreover, the whole purpose of the DMCA safe harbors was to “provide certainty for copyright owners and Internet service providers with respect to copyright infringement liability online.”⁴⁹

The loophole theory would completely undermine that purpose. Other than the inadvertent “loophole” theory, there is no explanation for why Congress might have wanted such a gaping loophole in the DMCA safe harbors as a policy matter. There is simply no basis in either the statute or the legislative history to conclude that Congress felt that vicarious infringement was somehow worse than contributory infringement to

provided by DOHSA, it did so expressly. We are reluctant to read the much more ambiguous language of § 7, which states only that state law ‘remedies’ or ‘rights of action’ would not be ‘affected’ and which makes no provision for reconciling potentially conflicting state and federal measures of recovery, to have the same substantive effect as the explicit command of § 4.”); *Russello v. U.S.*, 464 U.S. 16, 23 (1983) (“[W]here Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion.”) (quoting *U.S. v. Wong Kim Bo*, 472 F.2d 720, 722 (5th Cir. 1972)).

⁴⁶ Lemley, *supra* note 4, at 104 n.23.

⁴⁷ S. Rep. 105-190, at 40 (1998) (emphasis added); H.R. Rep. No. 105-551(II), at 50 (1998) (emphasis added).

⁴⁸ S. Rep. 105-190, at 43 (emphasis added); *see* H.R. Rep. No. 105-551(II), at 53.

⁴⁹ S. Rep. 105-190, at 2; H.R. Rep. 105-551(II), at 49-50.

justify including the latter, but not the former, within the safe harbor. Instead, the “loophole” reading rests on the shaky premise that Congress effectively goofed up in drafting a bill that both the House and Senate committee reports thought would provide immunity to vicarious liability. While it is true that Congress sometimes errs in drafting legislation, one should not jump to such a conclusion when an alternative, reasonable interpretation exists.⁵⁰

4. *The “loophole” interpretation shifts the burden of proving vicarious liability to the defendant*

Another oddity produced by the “loophole” interpretation of the DMCA is that it would effectively shift the burden of proof for vicarious liability claims to the defendant whenever the DMCA safe harbors under subsections (c) and (d) are invoked. The DMCA safe harbors are affirmative defenses that must be proven by the defendant; often, the defense is invoked on summary judgment without any determination on proof of liability because the safe harbor can dispose of the case.⁵¹ So under the “loophole” theory, the plaintiff would not have to prove vicarious liability; instead, the ISP would have to prove a negative, namely, that it did *not* commit vicarious liability.

Although Congress has the power to shift the traditional burden of proof in copyright cases, it is hard to imagine that Congress would have done so by choosing such an indirect, convoluted way. In an analogous situation, in interpreting the fair use defense in trademark cases, the Supreme Court rejected a similar interpretation of the Lanham Act that would have shifted the burden of proof on likelihood of confusion—a core element of trademark claims—to the defendant whenever fair use was invoked.⁵² The Court’s analysis on this point is particularly instructive:

Finally, a look at the typical course of litigation in an infringement action points up the incoherence of placing a burden to show nonconfusion on a defendant. If a plaintiff succeeds in making out a prima facie case of trademark infringement, including the element of likelihood of consumer confusion, the defendant may offer rebutting evidence to undercut the force of the plaintiff’s evidence on this (or any) element, or raise an affirmative defense to bar relief even if the prima facie case is sound, or do both. But it would make no sense to give the defendant a defense of showing affirmatively that the plaintiff cannot succeed in proving some element (like confusion); all the defendant needs to do is to leave the factfinder unpersuaded that the plaintiff has carried its own burden on that point. A defendant has no need of a court’s true belief when agnosticism

⁵⁰ See generally *Unites States v. Turkette*, 452 U.S. 576, 580 (1981) (avoid interpretations that “lead to internal inconsistencies, an absurd result, or an interpretation inconsistent with the intent of Congress”); see also *City of Columbus v. Ours Garage & Wrecking Serv., Inc.*, 536 U.S. 424, 449 n.4 (2002) (Scalia, J., dissenting) (recognizing “rule that a statute should not be interpreted to produce absurd results”); *U.S. v. X-Citement Video, Inc.*, 513 U.S. 64, 82 (1994) (Scalia, J., dissenting) (discussing “scrivener’s error” doctrine and application to statutes where “meaning genuinely intended but inadequately expressed”); *Public Citizen v. U.S. Dep’t of Justice*, 491 U.S. 440, 453 (1989).

⁵¹ See *UMG Recordings, Inc. v. Veoh Networks, Inc.*, No. CV 07-5744 AHM, 2008 WL 5423841, at *1 (C.D. Cal. Dec. 29, 2008) (“affirmative defense under the Digital Millennium Copyright Act’s ... ‘safe harbor’ provisions”).

⁵² *KP Permanent Make-Up, Inc. v. Lasting Impression I, Inc.*, 549 U.S. 111, 119-20 (2004).

will do. Put another way, it is only when a plaintiff has shown likely confusion by a preponderance of the evidence that a defendant could have any need of an affirmative defense, but under Lasting's theory the defense would be foreclosed in such a case. "[I]t defies logic to argue that a defense may not be asserted in the only situation where it even becomes relevant." Nor would it make sense to provide an affirmative defense of no confusion plus good faith, when merely rebutting the plaintiff's case on confusion would entitle the defendant to judgment, good faith or not.⁵³

The same criticism applies to "loophole" reading of the DMCA safe harbors. It is highly doubtful that Congress, in a "fit of terse drafting," meant to shift the burden of proof of vicarious liability in the DMCA safe harbors by oblique, roundabout language.⁵⁴ The legislative history indicates the exact opposite.⁵⁵

D. The Proper Interpretation: The DMCA Safe Harbors Provide Partial Immunity from Some, but Not All, Vicarious Infringement Claims

What then is the proper understanding of the DMCA's language "*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*"?

1. The DMCA's partial immunity from vicarious infringement

As explained above, the text of the DMCA is different from the common law standard of vicarious liability. Accordingly, the DMCA should not be interpreted to be the same as the common law standard. The term "receive a financial benefit *directly attributable* to the infringing activity" requires a closer causal connection between the infringing activity and the ISP's actual receipt of a financial benefit. It must be "directly attributable" to the infringing activity, which is a higher level of proof and causation than required under the common law.

In other words, Congress intended to disqualify some, but not all, forms of vicarious infringement—namely, the more egregious kinds—from the DMCA safe harbors. Although Congress did not describe the safe harbors in this way, I shall call this interpretation a *qualified immunity* or *partial immunity* reading of the DMCA. It is qualified in two senses: (i) ISPs have to *qualify* for the safe harbor by meeting certain requirements specified in the statute, and (ii) some forms of vicarious infringement (and also contributory infringement) are given immunity, while others (the more egregious forms) are not.⁵⁶ If the vicarious infringement resulted in the ISP "receiv[ing] a financial

⁵³ *Id.* at 120 (internal citations omitted).

⁵⁴ *Id.* at 118.

⁵⁵ See H.R. Rep. 105-551(I), at 26 ("While the burden of proving the elements of direct or contributory infringement, or vicarious liability, rests with the copyright owner in a suit brought for copyright infringement, a defendant asserting this exemption or limitation as an affirmative defense in such a suit bears the burden of establishing its entitlement.").

⁵⁶ Qualified immunity is best known as a doctrine for government officials who violate federal constitutional rights; such officials receive immunity if they did not violate "clearly established law" at the time of the violation. See *Harlow v. Fitzgerald*, 457 U.S. 800 (1982). I do not mean to suggest that Congress considered the qualified immunity doctrine from constitutional law as a basis for drafting the

benefit directly attributable to the infringing activity,” and if the ISP “has the right and ability to control such activity,” the DMCA safe harbors do *not* apply to immunize the ISP.

In essence, Congress chose to require proof of both (i) a closer causal connection—“directly attributable”—between the ISP’s alleged financial benefit and the third-party’s infringing activity and (ii) a greater level of actualized financial benefit or gains that are actually “receive[d]” by the ISP as a direct result of the infringement. I would characterize these circumstances as requiring evidence that the ISP actually received “ill-gotten gains” directly from the infringing activity of third parties, to borrow the lingo from unjust enrichment. In such case, immunity from monetary damages under the DMCA safe harbor would make little sense, since the ISP would have directly profited financially from infringing activity in a manner that is easy to trace back to the infringement. The ISP should not be able to profit from its ill-gotten gains.

This reading is supported by consideration of other federal statutes or laws in which “directly attributable” is used. In other areas of law, the language “directly attributable” is often used to describe a direct causal connection between certain conduct and resulting revenues or damages.⁵⁷ For example, the Age Discrimination Employment Act (ADEA) allows the court to award a prevailing plaintiff “attorney’s fees and costs demonstrated to be *directly attributable* only to the pursuit of a claim under section 2000e-2(m) of this title.”⁵⁸ Likewise in § 1983 claims, a municipality can be held liable for an officer’s conduct that violates constitutional rights only if the conduct is “directly attributable to the city’s policy or custom.”⁵⁹ A “direct attribution” requirement is often used to signal a greater causal connection before recovery of damages is allowed.

In the Copyright Act, the basic damages provision allows for recovery of “any profits of the infringer that are *attributable* to the infringement and are not taken into account in computing the actual damages,” under a burden-shifting scheme in which the plaintiff must offer proof of the infringer’s gross revenue, and then the burden shifts to the defendant to prove “her deductible expenses and the elements of profit *attributable* to factors other than the copyrighted work.”⁶⁰ The use of “directly” attributable in the DMCA safe harbor arguably implies an even greater showing of causation in the safe harbor than required under the basic damages provision for a copyright claim. Requiring proof of direct attribution for damages effectively serves as a way to limit the scope of

DMCA. Instead, I draw this analogy to a well-known kind of immunity, in order to illuminate how I believe the DMCA safe harbors operate in an analogous manner as a form of partial immunity to ISPs. To draw the analogy to constitutional law, officials are immunized from suits for violations of constitutional rights, but not the most egregious violations when they violated “clearly established law.”

⁵⁷ See, e.g., *Heck v. Humphrey*, 512 U.S. 477, 487 n.6 (1994) (state prisoner may not bring § 1983 claim “if a judgment in favor of the plaintiff would necessarily imply the invalidity of his conviction,” such as where he “seek[s] damages directly attributable to conviction or confinement”); *U.S. v. ASCAP*, No. Civ.A. 41-1395 (WCC), 2008 WL 1967722, at*56 (S.D.N.Y. April 30, 2008) (revenue “directly attributable” to different types of music uses online).

⁵⁸ 42 U.S.C. § 2000e-5(g)(2)(B) (emphasis added).

⁵⁹ *Fogel v. Collins*, 531 F.3d 824, 834 (9th Cir. 2008); see *Piotrowski v. City of Houston*, 237 F.3d 567, 578 (5th Cir. 2001).

⁶⁰ 17 U.S.C. § 504 (emphasis added).

liability to what damages the plaintiff has actually proven to have directly resulted from the illegal or tortious conduct, instead of indirect damages or speculative theories of resulting damages.⁶¹

2. *Structural analysis*

Other parts of the DMCA safe harbors support my interpretation. First, courts have interpreted the DMCA’s requirement of a “right and ability to control such [infringing activity]” in subsections (c) and (d) in a more limited or restrictive way than the common law standard under vicarious liability. Second, the DMCA safe harbors in subsections (c) and (d) also provide *partial or qualified* immunity from contributory infringement claims. Thus, because both of these requirements are contained in the same subsections, the other requirement of subsections (c) and (d) at issue here—“receive a financial benefit *directly attributable* to the infringing activity”—should be read consistently with these two other requirements as recognizing a form of partial or qualified immunity under the safe harbor.

i. DMCA standard of “right and ability to control such activity” has been interpreted more narrowly than vicarious liability standard

The DMCA safe harbor establishes a qualified immunity to vicarious liability in the other part of § 512(c)(1)(B)—the limitation that the financial benefit arise “in a case in which the service provider has the right and ability to control such activity.”⁶² If the service provider maintains no such right or ability, the whole financial benefit prong simply drops out of the picture for the DMCA safe harbor. Even though the similarity of language between this section and the common law standard of vicarious liability is even closer here than in the financial benefit prong of § 512(c)(1)(B), courts have already interpreted the DMCA standard of “right and ability to control such activity” in a more restrictive manner than its vicarious liability counterpart.

Specifically, a website’s ability to remove materials posted by third parties does *not* satisfy the “right and ability to control” under the DMCA safe harbors because such power is necessary for a website to satisfy the basic requirement of “takedown” under the DMCA.⁶³ The leading case is *Hendrickson v. eBay, Inc.*, in which the district court explained the reasons for interpreting the DMCA more narrowly:

⁶¹ See, e.g., *Corporate Healthcare Financing, Inc. v. BCI Holdings*, 444 F. Supp. 2d 423, 430-31 (D. Md. 2006) (“the litigation of BCI’s RICO claims would involve precisely the kind of unmanageable litigation and proof problems the *Anza* court meant to prevent. It would be extremely difficult to calculate how much of BCI’s lost profits might be directly attributable to the scheme rather than to a host of other reasons, compared to the relative ease of determining whatever amount of money Performax and NAHP unlawfully withheld from their customers”).

⁶² 17 U.S.C. § 512(c)(1)(B).

⁶³ See *Tur v. YouTube, Inc.*, 2007 WL 1893635, at *3 (C.D. Cal. 2007) (“The ‘right and ability to control’ infringing activity, as the concept is used in the DMCA, has been held to mean ‘something more’ than just the ability of a service provider to remove or block access to materials posted on its website or stored in its system.”); *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090 (W.D. Wash. 2004); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1181 (C.D. Cal. 2002); *Costar*, 164 F.

First, the “right and ability to control” the infringing activity, as the concept is used in the DMCA, cannot simply mean the ability of a service provider to remove or block access to materials posted on its website or stored in its system. To hold otherwise would defeat the purpose of the DMCA and render the statute internally inconsistent. The DMCA specifically requires a service provider to remove or block access to materials posted on its system when it receives notice of claimed infringement. *See* 17 U.S.C. §§ 512(c)(1)(C). The DMCA also provides that the limitations on liability *only* apply to a service provider that has “adopted and reasonably implemented ... a policy that provides for the termination in appropriate circumstances of [users] of the service provider’s system or network who are repeat infringers.” 17 U.S.C. § 512(i)(1)(A). 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.⁶⁴

Other courts that have considered the issue have all agreed with the *Hendrickson* court’s analysis.⁶⁵

The *Hendrickson* approach departs from the common law. How so? Traditional vicarious liability cases might well find that a website’s ability to terminate its users’ accounts and remove any user content the website finds inappropriate satisfies the “right and ability to control” requirement of vicarious liability.

For example, in the seminal case of *Shapiro, Bernstein & Co. v. Green Co.*, the court found that a department store’s contractual ability to supervise the conduct of an independent contractor who sold records within its store was enough to constitute “right and ability to supervise” for vicarious liability.⁶⁶ The court believed that its ruling would “simply encourage” the store to police the independent contractor as the store had the power to do.⁶⁷ The traditional “dance hall” cases in which vicarious liability has been found present an even more expansive view—in these cases, the dance hall might not even have any control over the selection of music played, but still be found vicariously liable.⁶⁸ Under this well-established case law, every website on the Internet that hosts material of third parties would be deemed to have the “right and ability to control” under the DMCA. That also might be the result under the Ninth Circuit’s analysis in *Fonovisa* and *Napster*, both of which found a right and ability to control infringing activity based

Supp. 2d at 704, *aff’d on other grounds*, 373 F.3d 544 (4th Cir. 2004); *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001); *see also* *Hendrickson v. Amazon.com, Inc.*, 298 F. Supp. 2d 914, 916 (C.D. Cal. 2003) (recognizing Amazon qualified for DMCA safe harbor giving immunity from vicarious infringement).

⁶⁴ *Hendrickson*, 298 F. Supp. 2d at 916.

⁶⁵ *See, e.g.*, *Io Group, Inc. v. Veoh Networks, Inc.*, -- F. Supp. 2d --, 2008 WL 4065872, at *16 (N.D. Cal. Aug. 27, 2008); *Tur v. YouTube, Inc.*, No. CV 06-4436 FMC, 2007 WL 1893635, at *3 (C.D. Cal. June 20, 2007); *Corbis Corp.*, 351 F. Supp. 2d at 1110; *Cybernet Ventures*, 213 F. Supp. 2d at 1181-82; *Costar*, 164 F. Supp. 2d at 704.

⁶⁶ *Shapiro, Bernstein & Co. v. H.L. Green Co.*, 316 F.2d 304, 308 (2d Cir. 1963).

⁶⁷ *Id.*

⁶⁸ *See, e.g.*, *Dreamland Ball Room v. Shapiro, Bernstein & Co.*, 36 F.2d 354, 355 (7th Cir. 1929).

on the respective defendant's contractual and actual ability to police its site and facilities for infringement.⁶⁹

However, the courts have rejected this approach to “right and ability to control” the third-party infringing activity under the DMCA. This growing line of case law might be characterized as requiring that that ISP have a level of *direct* control over the specific third-party activity in question—e.g., serving as an editor of content—that is greater than the ISP's general technological control over its website and its contractual ability to terminate accounts in a user agreement.

ii. *DMCA safe harbors establish partial immunity from contributory infringement*

My interpretation of § 512(c)(1)(B)'s relationship to vicarious liability is also supported by a structural analysis of the remaining parts of subsection (c). Subsection (c)(1)(A) deals with contributory infringement, especially the knowledge element, and effectively acts in a parallel manner to provide immunity from some, but not all, forms of contributory infringement.⁷⁰ For example, under traditional standards of copyright law, contributory infringement would be easily established if an ISP provided the “site and facilities” for third-party infringement on a website that stored third-party materials and knew that its users were engaging in infringing activity.⁷¹ However, the DMCA provides immunity to the ISP if, upon obtaining such knowledge, it “acts expeditiously to remove, or disable access to, the material” that is infringing.⁷² This is a form of qualified immunity because the ISP would not fall within the safe harbor if it acted too slowly or did nothing at all. The DMCA thus immunizes the ISP from some, but not all, forms of contributory infringement.

3. *Legislative History*

Legislative history confirms my reading. In several passages, both the Senate and the House Committees analyzed the “receive a financial benefit directly attributable” language. Yet nowhere did the committee reports ever suggest that Congress meant to codify a common law standard. Instead, the reports indicate the opposite.

At the outset of the Senate Report, the Judiciary Committee expressed a clear intention to *avoid* analyzing the “evolving” case law of secondary liability, stating:

There have been several cases relevant to service provider liability for copyright infringement. Most have approached the issue from the standpoint of contributory and

⁶⁹ See *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1023-24 (9th Cir. 2001) (“Napster ... has the ability to locate infringing material listed on its search indices, and the right to terminate users' access to the system.”); *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 262 (9th Cir. 1996) (“Cherry Auction had the right to terminate vendors for any reason whatsoever and through that right had the ability to control the activities of vendors on the premises.”).

⁷⁰ 17 U.S.C. § 512(c)(1)(A).

⁷¹ See *Fonovisa*, 76 F.3d at 264.

⁷² 17 U.S.C. § 512(c)(1)(A)(iii).

vicarious liability. *Rather than embarking upon a wholesale clarification of these doctrines, the Committee decided to leave current law in its evolving state and, instead, to create a series of ‘safe harbors,’ for certain common activities of service providers. A service provider which qualifies for a safe harbor, receives the benefit of limited liability.*⁷³

Later, the Senate Report indicates that “Section 512 is *not* intended to imply that a service provider is or is not liable as an infringer either for conduct that qualifies for a limitation of liability or for conduct that fails to so qualify.”⁷⁴ These statements are significant for two reasons. First, the Judiciary Committee recognized that the case law regarding vicarious and contributory infringement against ISPs was still “evolving.” As such, the case law may have been perceived as a moving target, and perhaps in need of “clarification.” Second, the Committee chose not to meddle with the “evolving” standards of secondary liability in copyright law, but instead to create the DMCA safe harbors. It is quite clear that the Judiciary Committee thought the DMCA safe harbors and secondary liability should be treated as two *separate* issues. Given this legislative history, the loophole reading becomes even more dubious. By all indications, the Committee did *not* view the DMCA safe harbors as somehow dependent on the “evolving” standards of secondary liability. If anything, these statements suggest the exact opposite—instead of adopting the “evolving” standards of vicarious liability that it decided to “leave” aside, Congress chose to create safe harbors *separate* from those standards.⁷⁵

The Senate Report later takes a view of “directly attributable” that is more restrictive than how courts have understood the “financial benefit” prong under vicarious liability:

Subsection (c)(1)(B) sets forth the circumstances under which a service provider would lose the protection of subsection (c) by virtue of its benefit from and control over infringing activity. 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.*⁷⁶

In these examples, the Senate required a specific showing that any fees gained were directly tied to infringing activity. This is a fairly high level of attribution.

⁷³ S. Rep. 105-190, at 19 (1998).

⁷⁴ *Id.* (emphasis added).

⁷⁵ *See also id.* (“Rather, the limitations of liability apply if the provider is found to be liable under existing principles of law.”).

⁷⁶ *Id.* at 44-45.

Like the Senate Committee, the House Committee on the Judiciary also viewed the case law on secondary liability as “evolving.” But the House Committee took a more express view on how the DMCA safe harbors *change* existing case law by making it “somewhat more difficult to satisfy” the liability standards by creating safe harbors.

Title II of this bill codifies the core of current case law dealing with the liability of on-line service providers, while narrowing and clarifying the law in other respects. It offers the advantage of incorporating and building on those judicial applications of existing copyright law to the digital environment that have been widely accepted as fair and reasonable. * * *

As to direct infringement, liability is ruled out for passive, automatic acts engaged in through a technological process initiated by another. Thus, the bill essentially codifies the result in the leading and most thoughtful judicial decision to date: *Religious Technology Center v. Netcom On-line Communications Services, Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995). In doing so, it overrules those aspects of *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993), insofar as that case suggests that such acts by service providers could constitute direct infringement, and provides certainty that Netcom and its progeny, so far only a few district court cases, will be the law of the land.

As to secondary liability, the bill changes existing law in two primary respects: (1) no monetary relief can be assessed for the passive, automatic acts identified in *Religious Technology Center v. Netcom On-line Communications Services, Inc.*; and (2) the current criteria for finding contributory infringement or vicarious liability are made clearer and *somewhat more difficult to satisfy*.⁷⁷

In the last sentence, the House Report clearly indicates an intent to treat the DMCA safe harbors *differently* than the common law standards of secondary liability. Thus, to the extent Congress borrowed common-law concepts of secondary liability, they are “somewhat more difficult to satisfy” under the DMCA. If that statement were not clear enough, the House Report goes on to state: “[T]he provision *modifies* and clarifies the knowledge element of contributory infringement *and the financial benefit element of vicarious liability*. *Even if a provider satisfies the common-law elements of contributory infringement or vicarious liability, it will be exempt from monetary liability* if it satisfies the criteria in subparagraphs (A) and (B).”⁷⁸

The House Report used the same examples of what does and does not constitute a “financial benefit directly attributable to” infringing activity as contained in the Senate Report.⁷⁹ Although the Senate and House reports did not compare its standard with

⁷⁷ H.R. Rep. 105-551(I), at 11 (Judiciary Committee).

⁷⁸ *Id.* at 25. *See also id.* at 25-26 (“The financial benefit standard in subparagraph (B) is intended to codify and clarify the direct financial benefit element of vicarious liability as it has been interpreted in cases such as *Marobie-FL, Inc. v. National Association of Fire Equipment Distributors*, -F. Supp.-(N.D. Ill. 1997). As in *Marobie*, 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.”).

⁷⁹ *See id.* at 25-26; H.R. Rep. 105-551 (II), at 54 (Commerce Committee).

vicarious infringement cases, we can undertake such a comparison here. According to the Senate report, a flat fee charged and collected by an ISP from its users would *not* constitute “receiv[ing] a financial benefit directly attributable to the infringing activity.” By contrast, under vicarious liability standards as applied by the Ninth Circuit in *Fonovisa*, a flea market was found to have potentially received a “direct financial benefit” based on general admission fees, concession fees, and parking fees that were charged to any member of the public, regardless of whether they purchased bootlegged recordings at the flea market.⁸⁰ Although these general fees charged to any member of the public were enough for vicarious infringement, they would *not* be enough to constitute a “financial benefit directly attributable to the infringing activity” under the DMCA, in my view. As the Senate Report indicates, “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.*”

4. *Other examples of how the DMCA safe harbors are “somewhat more difficult to satisfy” than vicarious liability*

One can easily find other examples where the DMCA’s requirement of a “financial benefit directly attributable to the infringing activity” is different from the vicarious liability standard of financial benefit, and would produce a different outcome.

For example, in *Famous Music Corp. v. Bay State Harness Horse Racing & Breeding Association, Inc.*,⁸¹ a horse race track hired an independent contractor to provide music “[t]o entertain its patrons when they were not absorbed in watching the races.”⁸² Although the race track had not obtained an ASCAP license, it did instruct the independent contractor “*not* to play any ASCAP copyrighted music.”⁸³ But, on two different days, the independent contractor did so anyway.⁸⁴ The district court found the horse track liable for the activities of the independent contractor,⁸⁵ and the First Circuit affirmed.⁸⁶

However, under my reading of the DMCA safe harbors, even though the race track was vicariously liable, the race track did *not* “receive a financial benefit directly attributable to the infringing activity” based simply on patronage of the race track. There was *no* evidence at all that patrons were paying admission fees or spending money at the race track in order to listen to music of any kind, whether unauthorized or under license. Presumably, people were paying the race track to make bets on the races! Therefore, the race track’s revenues would *not* be “directly attributable to the infringing activity.”

⁸⁰ *Fonovisa, Inc., v. Cherry Auction, Inc.*, 76 F.3d 259, 263 (9th Cir. 1996).

⁸¹ 554 F.2d 1213 (1st Cir. 1977).

⁸² *Id.* at 1214.

⁸³ *Id.* (emphasis added).

⁸⁴ *Id.*

⁸⁵ 423 F. Supp. 341, 344-45 (D. Mass. 1976).

⁸⁶ 554 F.2d at 1215.

Similarly, in the old Supreme Court case *Buck v. Jewell-La Salle Realty Co.*,⁸⁷ a hotel was found liable for wiring in radio broadcasts into each room and allowing its patrons to listen to the radio, which apparently included both authorized performances of different songs and several unauthorized performances of the plaintiff's song played by a third-party radio station that selected the music.⁸⁸ These facts do not establish that the hotel "receive[d] a financial benefit directly attributable to the infringing activity" of the third-party radio station. The hotel earned no extra profit or fees from playing the radio, which happened to include some unauthorized performances by the third party. In such case, it would be purely speculative to say that the hotel even received an *indirect* financial benefit from the radio station's infringement, since it is not even clear that the hotel guests were seeking the infringing music or even liked the particular song played.

By contrast, *Napster* presents a harder case. The music-file sharing service Napster offered its services all for free.⁸⁹ Since no fees were involved or ever received by Napster, one could plausibly argue that Napster never actually "receive[d] a financial benefit directly attributable to the infringing activity" because Napster never actually made any money from its users' illegal activity. However, under vicarious infringement standards, the district court found a financial benefit based on *potential future revenues* from establishing a user-based comprised of users all looking for free, infringing music.⁹⁰ Napster had a "direct financial interest" in infringing music files because it acted as a "draw" for users to Napster's site.⁹¹

Would this putative financial benefit be enough to satisfy the DMCA standard? Perhaps, but only in an extreme set of facts like *Napster*. Although debatable, one could argue, to borrow the Senate Report's language, that the whole value of the Napster service was "in providing access to infringing material"⁹² since virtually all of its users were purportedly sharing unauthorized files. Thus, to the extent that the Napster business could be valued as a startup by accepted accounting methods and some portion of the value directly attributed to Napster's providing access to infringing activity, such proof might well be enough to constitute a "financial benefit directly attributable to the infringing activity."⁹³

Napster, though, is a pretty extreme case in which an entire business was purportedly designed around illegal sharing of music, as evidenced by internal company

⁸⁷ 283 U.S. 191 (1931).

⁸⁸ *Id.* at 198-99.

⁸⁹ *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1023 (9th Cir. 2001).

⁹⁰ *A&M Records, Inc. v. Napster, Inc.*, 114 F. Supp. 2d 896, 902 (N.D. Cal. 2000), *aff'd in part and rev'd in part*, 239 F.3d 1004 (9th Cir. 2001).

⁹¹ *Id.* at 921, *aff'd in relevant part*, 239 F.3d 1004, 1023 (9th Cir. 2001) ("Financial benefit exists where the availability of infringing material 'acts as a 'draw' for customers.'").

⁹² S. Rep. 105-190, at 44-45 (1998); *see also* H.R. Rep. 105-551(II), at 54.

⁹³ Napster did assert a DMCA safe harbor defense. It is not clear whether Napster followed the other prerequisites of the DMCA safe harbor, and before a trial was held on Napster's DMCA safe harbor defense, it went bankrupt. *See A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1025 (9th Cir. 2001) (noting questions about Napster's DMCA defense but sending it back for trial).

documents.⁹⁴ Courts must be careful not to relax the DMCA standard of “receive a financial benefit directly attributable to the infringing activity” by allowing the *Napster* court’s “financial draw” analysis to extend too far. A company’s development of a user-base should not be, in itself, evidence that the company “receive[d] a financial benefit directly attributable to” any infringing activity that might have occurred on the site. Otherwise, every single commercial website would fall outside of the DMCA safe harbors.

II. Decoding the “Red Flags” Theory of Liability

Another key issue regarding the DMCA safe harbors concerns the so-called “red flags” theory. Beyond receiving a DMCA notice from a copyright holder, under what circumstances must an ISP remove potentially infringing material in order to invoke the DMCA safe harbor? The basic answer is easy to state: a duty arises if the ISP has either *actual knowledge* of the infringing material on its site, or is “aware of facts or circumstances from which infringing activity is apparent.”⁹⁵ However, the difficulty lies in determining the latter, “awareness of infringement” prong. Copyright holders have argued that such awareness should be found to exist based on “red flags” created by the existence of other infringing activity on a site. This Part explains why the few courts that have considered the issue have correctly applied a very high standard of proof to satisfy the “awareness of infringement” prong or establish the so-called “red flags” theory.

A. Relevant Text of the DMCA safe harbor

Both the hosting safe harbor in § 512(c) and the safe harbor for information location tools in § 512(d) contain several provisions dealing with the ISP’s knowledge of infringing activity. Although the provision is quoted above, it is worth repeating it in full here for convenience of the reader:

(c) Information residing on systems or networks at direction of users.--

(1) In general.--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--

(A)(i) *does not have actual knowledge that the material or an activity using the material on the system or network is infringing;*

(ii) *in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or*

(iii) *upon obtaining such knowledge or awareness, acts expeditiously to remove,*

⁹⁴ *Napster*, 239 F.3d at 1020 n.5 (discussing evidence of knowledge of infringement by Napster co-founder and executives).

⁹⁵ 17 U.S.C. § 512(d)(1).

or disable access to, the material;

(B) 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; and

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

The same language in § 512(c)(1)(A) and (C) can be found in § 512(d)(1) and (3), which sets forth the requirements for the safe harbor for activity involving location tools.⁹⁶

These “knowledge” subsections effectively qualify the knowledge element of contributory infringement. Under contributory liability, a defendant can be liable if he knew or had reason to know of another’s direct infringement and materially contributed to it.⁹⁷ Under the DMCA safe harbor, however, knowledge of infringing activity and material contribution are not dispositive; an ISP can possess knowledge of a third party’s direct infringement, but still fall within the safe harbor by “act[ing] expeditiously to remove, or disable access to, the material.”⁹⁸

This is known as the DMCA “notice and take-down” procedure, which is the most common way that alleged copyright infringements are resolved online. An ISP can be found to possess the requisite knowledge activating the ISP’s duty to “take down” material by the copyright holder’s submission of a DMCA notice of claimed infringement to the ISP as set forth under the DMCA.⁹⁹

But the DMCA safe harbor also requires such takedown if the ISP has either (i) actual knowledge of infringing material or (ii) “aware[ness] of *facts or circumstances from which infringing activity is apparent*” as set forth in subsection (A).¹⁰⁰ It is this latter, more nebulous section dealing with “awareness” that creates some uncertainty for ISPs and copyright holders.

B. When Is an ISP “Aware of Facts from Which Infringing Activity Is Apparent”?

So when does an ISP have a sufficient level of “aware[ness] of facts from which infringing activity is apparent,” thus giving rise to a duty to take down the material to fall within the DMCA safe harbor? As with all knowledge-based questions, a lot will depend on facts of each case. The Senate Judiciary Committee report indicates that “aware[ness]” be judged both *subjectively* (the ISP’s actual state of mind) and *objectively*, asking “whether infringing activity would have been apparent to a reasonable

⁹⁶ See 17 U.S.C. § 512(d)(1), (d)(3).

⁹⁷ See *NCR Corp. v. Korala Assoc., Ltd.*, 512 F.3d 807, 816 (6th Cir. 2008).

⁹⁸ See 17 U.S.C. § 512(c)(1)(C).

⁹⁹ 17 U.S.C. § 512(c)(3).

¹⁰⁰ *Id.* § 512(c)(1).

person operating under the same or similar circumstances.”¹⁰¹ The House report agrees.¹⁰²

1. Plain Language

A close textual analysis provides some indication that Congress intended to establish a very high standard of knowledge. The ISP must be “aware of facts or circumstances from which *infringing activity is apparent*.” It is not enough, in other words, that the facts suggest potential or possible infringement. It is not enough that the facts might raise a suspicion of infringement. There must be actual infringement occurring and it must be “*apparent*” from the facts or circumstances.

Under a dictionary definition, “apparent” means “(1) readily seen; exposed to sight; open to view; visible; (2) capable of being easily perceived or understood; plain or clear; obvious.”¹⁰³ Thus, one is “aware of facts from which infringing activity is apparent,” when it is “plain, clear, or obvious” from the facts that infringement is occurring.¹⁰⁴ As discussed later below, the Committee reports confirm Congress’s intent to require a high standard of knowledge.

2. Structural analysis of the DMCA

The overall structure of the DMCA safe harbors also supports adopting a high standard of awareness of “obvious” or “blatant” infringement.

First, the whole point of a safe harbor is to provide a clear path for members of the public to avoid liability. In enacting the DMCA safe harbors, Congress hoped to “provide[] *greater certainty* to service providers concerning their legal exposure for infringements that may occur in the course of their activities.”¹⁰⁵ Requiring a high level of proof to establish that an ISP was “aware of facts from which infringing activity is apparent” serves the whole purpose of having a safe harbor. A low standard, however, would invite constant litigation against Internet companies, given how easy it would be to allege that they were “aware of facts from which infringing activity is apparent.” Every website that has implemented the notice-and-takedown procedure of the DMCA probably has run into problems of alleged copyright infringement, which then could be used as the basis for an allegation that the ISP was “aware of facts from which infringing activity is apparent.”

Second, the DMCA expressly states that an ISP does *not* have any affirmative duty to “monitor[] its service or [to] *affirmatively seek[] facts indicating infringing*

¹⁰¹ S. Rep. 105-190, at 44.

¹⁰² H.R. Rep. 105-551(II), at 51.

¹⁰³ RANDOM HOUSE WEBSTER’S UNABRIDGED DICTIONARY 100 (2d ed. 2001).

¹⁰⁴ This use of “apparent” is not to be confused with the different, third meaning of “apparent”: “(3) according to appearances, initial evidence, incomplete results, etc.; ostensible rather than actual.” *Id.* As explained below, the legislative history does not support application of this meaning.

¹⁰⁵ S. Rep. 105-190, at 40 (emphasis added); *see also* H.R. Rep. 105-551(II), at 49-50.

activity.”¹⁰⁶ This provision helps to ensure that ISPs can continue to rely on automated systems that are commonplace on the Internet. Congress did not want to turn ISPs into censors of material or to create perverse incentives for ISPs to remove indiscriminately vast amounts of material for fear of copyright lawsuits. Congress realized that the question of what constitutes copyright infringement is so often difficult, if not impossible, to determine outside of court. Both the Senate and the House committee reports indicate the DMCA was drafted so as to avoid imposing a duty on ISPs to “investigate possible infringements, monitor its service, or *make difficult judgments as to whether conduct is or is not infringing*.”¹⁰⁷

Another key component of the DMCA is the notice-and-takedown procedure. Congress chose to place some of the burden on copyright holders to provide notice of claimed infringement and some of the burden on ISPs to take down such material, in a spirit of cooperation.¹⁰⁸ Congress understood the value of the decentralized nature of the Internet, particularly in allowing the widespread dissemination of speech. The notice-and-takedown process serves important First Amendment goals because it avoids the specter of ISPs indiscriminately censoring speech due to fears of copyright lawsuits by requiring copyright holders to indicate, under penalty of perjury, when and where they believe their works have been infringed.¹⁰⁹ As the Ninth Circuit explained: “This requirement is not superfluous. Accusations of alleged infringement have drastic consequences: A user could have content removed, or may have his access terminated entirely. If the content infringes, justice has been done. But if it does not, speech protected under the First Amendment could be removed.”¹¹⁰

Finally, § 512(j), the injunction provision in the DMCA, allows courts to enjoin, under certain conditions, an ISP that falls within the safe harbor.¹¹¹ All of these

¹⁰⁶ 17 U.S.C. § 512(m).

¹⁰⁷ S. Rep. No. 105-190, at 32; H.R. Rep. No. 105-551(II), at 44 (emphasis added); *see also* Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1101(W.D. Wash. 2004) (“Given the complexities inherent in identifying and defining online copyright infringement, § 512(i) does not require a service provider to decide, *ex ante*, the specific types of conduct that will merit restricting access to services.”).

¹⁰⁸ S. Rep. 105-190, at 40 (“Title II 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.”); H.R. Rep. No. 105-551(II), at 49 (same).

¹⁰⁹ *See* 17 U.S.C. § 512(c)(3).

¹¹⁰ *Perfect 10 v. CCBill LLC*, 488 F.3d 1102, 1112 (9th Cir. 2007). Some scholars have criticized the notice-and-takedown procedure as lending itself to questionable claims of infringement that lead to potentially unwarranted removal of legitimate materials online. *See* Jennifer M Urban & Laura Quilter, *Efficient Process or “Chilling Effects”? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 621, 679-80 (2006); Lemley, *supra* note 4, at 114-15.

The DMCA provides some relief against unjustified DMCA notices. First, the person whose material was removed has the right to file a “counter notification” to the ISP, which then obligates the ISP to re-post the material within 14 days unless the copyright holder notifies the ISP that it has filed an action seeking a court order. 17 U.S.C. § 512(g). Also, the DMCA creates a cause of action against anyone who has knowingly misrepresented in a DMCA notice. *Id.* § 512(f). Even if some DMCA notices involve only weak or questionable claims of infringement, copyright holders often complain that the removal of material online is ineffectual because it is so easy for someone to re-post the exact same material.

¹¹¹ 17 U.S.C. § 512(i).

conditions require great specificity in identifying the person engaging in infringing activity or the particular location of the infringing material online.¹¹² A broad injunction to stop infringement occurring generally on a website would not pass muster. Congress also specified four factors for courts to consider in issuing injunctions:

- (A) whether such an injunction, either alone or in combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider's system or network;
- (B) the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement;
- (C) whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations; and
- (D) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.¹¹³

Three of the four factors are concerned with not imposing significant or impracticable burdens on ISPs to try to stamp out infringement online. These several provisions further support requiring a high level of proof to establish an ISP is “aware of facts from which infringing activity is apparent.”

3. Legislative history: obvious infringement and “red flags”

The Senate and the House committee reports support this view. In order for infringing activity to be “apparent,” it must be “obviously” or “clearly” infringing, such as a well-known “pirate” site. The Reports explain this high standard in what is sometimes called the “red flags” theory:

Under this standard, 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*.

For instance, the copyright owner could show that the provider was aware of facts from which infringing activity was apparent if the copyright owner could prove that the location was *clearly, at the time the directory provider viewed it, a “pirate” site* of the type described below, where sound recordings, software, movies or books were available for unauthorized downloading, public performance or public display.* * *

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. Such pirate directories refer Internet users to sites that are *obviously infringing* because they typically use words such as “pirate,” “bootleg,” or slang terms in their uniform resource locator (URL) and header information to make their *illegal purpose obvious to the pirate directories and other Internet users*. Because the infringing nature

¹¹² *Id.*

¹¹³ *Id.* § 512(j)(2).

of such sites would be apparent *from even a brief and casual viewing*, safe harbor status for a provider that views such a site and then establishes a link to it would not be appropriate. Pirate directories do not follow the routine business practices of legitimate service providers preparing directories, and thus evidence that they have viewed the infringing site may be all that is available for copyright owners to rebut their claim to a safe harbor.¹¹⁴

The Committee Reports explain the important policy reason for choosing a high standard for “awareness of infringement.” The basic reason is that the whole question of infringement is so often difficult to determine outside of court, so Congress did not want to saddle Internet sites with the impossible burden of trying to differentiate what constitutes copyright infringement in the myriad of situations on the Internet.

In this way, the “red flag” test in section 512(d) strikes the right balance. *The common-sense result of this “red flag” test is that on-line editors and catalogers would not be required to make discriminating judgments about potential copyright infringement.* If, however, an Internet site is *obviously pirate*, then seeing it may be all that is needed for the service provider to encounter a “red flag.” A provider proceeding in the face of such a red flag must do so without the benefit of a safe harbor.¹¹⁵

The Nimmer treatise agrees with the soundness and sensibility of Congress’s approach.¹¹⁶

Finally, a “red flag” cannot exist based merely on the fact that infringement occurred in the past on the Internet service. As Jonathan Band has explained, the DMCA contemplates that Internet service providers will have to face infringement on their sites, and the DMCA safe harbors were never intended to allow only “one free pass” from liability.¹¹⁷

4. Cases

Only a few courts so far have considered whether an ISP was “aware of facts and circumstances from which infringing activity is apparent” under the so-called “red flags” theory. All have applied a high standard of particularized knowledge, consistent with the interpretation I have outlined above.

A leading case is *Perfect 10 v. CCBill*,¹¹⁸ which involved a copyright lawsuit brought by an adult magazine *Perfect 10* against CWIE, a webhosting service, and CCBill, an online payment service, that allegedly provided services to third-party websites that had infringing photos of *Perfect 10*.¹¹⁹ The Ninth Circuit rejected the

¹¹⁴ S. Rep. 105-190, at 48-49; H. Rep. 105-551, at 57-58.

¹¹⁵ S. Rep. 105-190, at 48-49; H. Rep. 105-551, at 57-58.

¹¹⁶ See 3 NIMMER & NIMMER, *supra* note 15, at 12B-04[A][2][a] (“The balance of this treatise attests to how difficult it can be to determine whether all the elements of infringement are present—from proper ownership and standing to lack of license (express or implied) to satisfaction of notice formalities (unless excused by national origin or otherwise), to the perennially murky issue of fair use, and beyond.”).

¹¹⁷ See Band, *supra* note 5, at 315-16.

¹¹⁸ 488 F.3d 1102 (9th Cir. 2007).

¹¹⁹ *Id.* at 1108.

plaintiff's assertions that "red flags" of infringement existed based on the fact that the defendants provided services to (i) two websites with domain names "illegal.net" and "stolencelebritypics.com," and (ii) several websites that allegedly provided services to hack password security measures on other websites.¹²⁰ The court concluded that the facts did not establish actual copyright infringement, much less defendants' knowledge of it, and there was no duty for ISPs to investigate further under the DMCA.¹²¹ For example, the domain names did not establish copyright infringement in themselves because the domain names with "illegal" or "stolen" could "be an attempt to increase their salacious appeal, rather than an admission that the photographs are actually illegal or stolen."¹²² The court held that the DMCA did "not place the burden of determining whether photographs are actually illegal on a service provider."¹²³

Another key case is *Corbis Corp. v. Amazon.com*.¹²⁴ Corbis was a distributor for licensed photographs and art images taken by photographers who had contracts with Corbis.¹²⁵ Over 230 copyrighted images were allegedly posted without Corbis's permission on third party websites hosted by Amazon under its "zShops" service, as well as on the Internet Movie Database (IMDb), which was owned by Amazon.¹²⁶ Instead of sending a DMCA notice to Amazon, Corbis sued.¹²⁷ In holding that Amazon fell within the DMCA safe harbor (for the majority of claims), the district court rejected Corbis's argument that Amazon had knowledge of "red flags" indicating infringement based on its general awareness that infringement could be taking place on zShops sites.¹²⁸ Citing the committee reports, the court held that Congress established a very high standard of "blatant" or "obvious" infringement that is clear "from even a 'brief and casual viewing.'"¹²⁹

The court elaborated on when infringement may be clear or blatant.¹³⁰ "[I]t requires, at a minimum, that a service provider who receives notice of a copyright violation be able to tell merely from looking at the user's activities, statements, or conduct that copyright infringement is occurring."¹³¹ That inquiry, moreover, must be tempered with possible fair use and other defenses that can be raised.¹³² In applying this standard, the district court rejected Corbis's argument that Amazon had knowledge of a "red flag" based on its receipt of 10 total DMCA notices against two different vendors on Amazon's zShops sites that provided photographs that allegedly infringed the copyrights of others.¹³³ The court explained:

¹²⁰ *Id.* at 1114.

¹²¹ *Id.*

¹²² *Id.*

¹²³ *Id.*

¹²⁴ 351 F. Supp. 2d 1090 (W.D. Wash. 2004).

¹²⁵ *Id.* at 1096.

¹²⁶ *Id.* at 1096-97.

¹²⁷ *Id.* at 1097.

¹²⁸ *Id.* at 1107-08.

¹²⁹ *Id.* (quoting H.R. Rep. No. 105-551, pt. 2, at 57).

¹³⁰ *Id.* at 1104-05.

¹³¹ *Id.* at 1105 (emphasis added).

¹³² *Id.*

¹³³ *Id.* at 1104.

[T]here is no evidence suggesting that Amazon would have been able to tell, merely by looking at the Famed & Framed and Posternow listings, that the posters and photos being sold infringed another's copyrights. Without some evidence from the site raising a red flag, Amazon would not know enough about the photograph, the copyright owner, or the user to make a determination that the vendor was engaging in blatant copyright infringement. *See* S. Rep. No. 105-190, p. 30 (merely being aware of "one or more well known photographs of a celebrity at a site" does not provide a service provider with knowledge of possible infringement).

Finally, although the DMCA safe harbors do not apply to trademark law, the recent trademark case of *Tiffany v. eBay* takes a very similar approach to answering the question of what level of knowledge of infringing activity on a website such as eBay must be present before the site has a duty to stop or correct the activity.¹³⁴ Just as in copyright law,¹³⁵ contributory infringement under trademark law requires that the defendant "know[s] or [has] reason to know" of the infringing activity.¹³⁶ The *Tiffany* court ruled that eBay's generalized knowledge that some infringing (third-party) activity took place on eBay's website was *insufficient* to satisfy the knowledge prong or to impose an affirmative duty for eBay to address the general problem, apart from eBay's undisputed remedial efforts once it had knowledge of specific instances of infringement.¹³⁷ In short, *specific knowledge* of a particular infringement—such as "written notice of a specific infringing event, providing the date, the event, and the location of the event"—is required before trademark law imposes a duty on the defendant to monitor its website.¹³⁸ That an Internet site generally knows that conduct on its site "might be" infringing is *not* enough to serve as the basis of knowledge of "specific instances of actual infringement."¹³⁹

C. Applying the Awareness Standard to YouTube and MySpace

To understand the proper understanding of the awareness standard under § 512(c)(1)(A), let's consider one common scenario from the video sharing context. Today, people are able to upload videos onto YouTube, MySpace Video, and a host of other sites. (Both YouTube and MySpace have been sued for copyright infringement based on their users' videos in several cases that are still ongoing.¹⁴⁰)

What happens if an employee of YouTube or MySpace randomly notices, on their respective sites, a thumb-nail image or screen shot of a video that contains the image of Jerry Seinfeld with the header "Seinfeld"? Thumb-nail images or still "screen shots" of videos are commonly used by video-sharing websites like YouTube and MySpace to give a snapshot of what content each video contains. The screen shots are usually generated

¹³⁴ *Tiffany Inc. v. eBay, Inc.*, 576 F. Supp. 2d 463, 508 (S.D.N.Y. 2008).

¹³⁵ *Id.* at 510 n.37.

¹³⁶ *Id.* at 508.

¹³⁷ *Id.* at 507-08.

¹³⁸ *Id.* at 509.

¹³⁹ *Id.* at 511; *see id.* at 511 ("Such general knowledge ... does not require eBay to take action to discontinue supplying its service to all those who *might* be engaged in counterfeiting.")

¹⁴⁰ *See* Lee, *supra* note 3, at 1513-14.

automatically from each video; some sites, like YouTube, allow the user to choose from among several automatically-generated screen shots. Imagine in our hypothetical that the screen shot of Jerry Seinfeld looks like a shot from his popular television show. Would the Seinfeld screen shot be a “red flag”?

No. Under my reading of the DMCA, the employee’s mere knowledge of a Jerry Seinfeld thumb-nail image or screen shot on the website would *not* constitute being “aware of facts from which infringing activity is apparent.” It is neither plain, clear, nor obvious that a mere screen shot of Jerry Seinfeld is copyright infringement. The problem with applying the “red flags” theory here is that the color of the flag is unclear—it may be pink, green, orange, white, or a variety of other colors.

Put simply, the copyright status of the Seinfeld video is unclear from the mere image of the screenshot. True, the video clip could be an unauthorized copy of part of a *Seinfeld* episode, or an unauthorized bootleg of a Jerry Seinfeld comedy routine performed in Vegas. But it also could be just a single photograph of Seinfeld spliced into a user-generated video, a random “teaser” thrown in the video to attract more views. It also could be a legitimate copy used for fair use purposes, such as a parody of Seinfeld. There’s also the possibility that the video clip could have been authorized by Jerry Seinfeld himself or the *Seinfeld* copyright holder for posting. In other words, infringement is not “apparent”—clear, plain, or obvious—from merely viewing the screen shot of Jerry Seinfeld, the title, and the username of the person who posted it. The DMCA does not obligate the ISP to “affirmatively seek[] facts indicating infringing activity,” so the ISP would be under no duty to investigate further.¹⁴¹

The scenario is similar to the one discussed in *Corbis*, in which the court rejected the notion that the photographs on a site provided a “red flag” of infringement. Also, the Senate and House reports both point to an analogous situation in which they found no obvious infringement:

Absent such “red flags” or actual knowledge, a directory provider would not be similarly aware merely because it saw one or more well known photographs of a celebrity at a site devoted to that person. The provider could not be expected, during the course of its brief cataloguing visit, 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.¹⁴²

The same predicament befalls the YouTube or MySpace employee in the Seinfeld scenario. Although imposing a duty for ISPs to look at just *one* Seinfeld video does not seem like much, hundreds of thousands of videos are uploaded each day on YouTube alone.¹⁴³ Requiring an ISP to review every video based on screen shots that could suggest infringement (or not) would effectively gut § 512(m)’s clear proscription against imposing a duty to monitor on ISPs.

¹⁴¹ 17 U.S.C. § 512(m)(1).

¹⁴² *Id.*

¹⁴³ See http://www.youtube.com/t/fact_sheet.

III. Rebooting the DMCA Safe Harbors for the Future

In the ten years following the DMCA's enactment, courts have decided less than twenty-five cases involving the DMCA safe harbors (some of which did not even render a final decision on the merits of the DMCA defense).¹⁴⁴ The relative lack of litigation is both a blessing and a curse. It is a blessing because Internet companies and web applications of all kinds have flourished, with a tremendous growth of user-generated content and speech activities online. As Professor Tim Wu aptly put it, the DMCA safe harbors are "the Magna Carta for Web 2.0."¹⁴⁵ No one can deny the tremendous success over the past decade in achieving the central goal of the DMCA safe harbors—"by 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."¹⁴⁶ The DMCA "facilitate[s] the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age."¹⁴⁷ The Internet of 2009 is light years beyond the Internet of 1998.

But the lack of litigation is also a curse because it allows ambiguities on seemingly basic issues about the scope of protection under the DMCA safe harbors to persist for long periods of time, and in a way that exposes Internet companies to

¹⁴⁴ Only 3 circuit courts of appeals (the Fourth, the Seventh, and the Ninth) have dealt with application of the DMCA safe harbors in a total of 8 cases with published decisions. *See* *Costar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544, 552 (4th Cir. 2004); *ALS Scan, Inc. v. RemarQ Communities, Inc.*, 239 F.3d 619, 622 (4th Cir. 2001); *In re Aimster Copyright Ltgn.*, 334 F.3d 643, 655 (7th Cir. 2003); *Perfect 10 Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1175 (9th Cir. 2007); *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1109 (9th Cir. 2007); *Rossi v. MPAA*, 391 F.3d 1000, 1003 (9th Cir. 2004); *Ellison v. Robertson*, 357 F.3d 1072, 1076 (9th Cir. 2004); *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1025 (9th Cir. 2001). I have excluded from this count cases dealing with the subpoena power under § 512(h).

Besides the cases listed above, the district courts (from only 6 different districts) have dealt with the application of the DMCA safe harbors in only 16 other cases by my count, not all of which finally adjudicated the DMCA defense. *See* *UMG Recordings, Inc. v. Veoh Networks, Inc.*, No. CV 07-5744 AHM, 2008 WL 5423841, at *7 (C.D. Cal. Dec. 29, 2008); *Arista Records LLC v. Usenet.com, Inc.*, No. 07 Civ. 8822(HB), 2008 WL 4974823, at *4 (S.D.N.Y. Nov. 24, 2008); *Lenz v. Universal Music Corp.*, No. C 07-3783 JF, 2008 WL 4790699, at *2 (N.D. Cal. Oct. 28, 2008); *Io Group, Inc. v. Veoh Networks, Inc.*, -- F. Supp. 2d --, 2008 WL 4065872 (N.D. Cal. Aug. 27, 2008); *Doe v. Geller*, 533 F. Supp. 2d 996, 1001 (N.D. Cal. 2008); *Tur v. YouTube, Inc.*, No. CV 06-4436 FMC, 2007 WL 1893635, at *3 (C.D. Cal. June 20, 2007); *Tur v. YouTube, Inc.*, No. CV 06-4436 FMC, 2007 WL 4947612, at *2 (C.D. Cal. June 20, 2007); *Parker v. Google, Inc.*, 422 F. Supp. 2d 492, 498 (E.D. Pa. 2006); *Field v. Google, Inc.*, 412 F. Supp. 2d 1106, 1124 (D. Nev. 2006); *Dudnikov v. MGA Ent., Inc.*, 410 F. Supp. 2d 1010, 1012 (D. Colo. 2005); *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1098 (W.D. Wash. 2004); *Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195, 1204-05 (N.D. Cal. 2004); *Hendrickson v. Amazon.com, Inc.*, 298 F. Supp. 2d 914, 916 (C.D. Cal. 2003); *Arista Records, Inc. v. MP3Board, Inc.*, No. 00 CIV. 4660, 2002 WL 1997918, at *8 (S.D.N.Y. Aug. 29, 2002); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1174 (C.D. Cal. 2002); *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1088 (C.D. Cal. 2001); *Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp. 2d 211, 217 (S.D.N.Y. 2000).

¹⁴⁵ Tim Wu, *Does YouTube Really Have Legal Problems*, SLATE, Oct. 26, 2006, at <http://www.slate.com/id/2152264/>.

¹⁴⁶ S. Rep. 105-190, at 8.

¹⁴⁷ *Id.* at 1-2.

potentially unjustified threats of copyright lawsuits. Uncertainty defeats the whole purpose of a safe harbor because companies are unable to identify the necessary steps to avoid liability. Parts I and II above have attempted to clear up two of the key ambiguities of the DMCA safe harbors. But these ambiguities, along with others, will persist until courts clarify them. And, unfortunately, we can expect other ambiguities to arise, given the way in which the technologies of the Internet rapidly develop and change. This final Part provides more general guidance and a set of principles for both courts and Congress on how the DMCA safe harbors can be made safe and workable in today's Internet age.

A. Principles for Making the DMCA Safe Harbors Safe

I offer several principles and proposals that can help the DMCA safe harbors work more efficiently, i.e., to make them truly “safe” harbors.

1. Loophole theories of the DMCA should be disfavored

First, in interpreting the DMCA safe harbors, courts should disfavor interpretations that create loopholes. Where the DMCA safe harbors are ambiguous, courts should disfavor an interpretation that threatens to create a loophole or otherwise severely undermine the whole concept of a safe harbor. Where a reasonable alternative interpretation exists, the court should adopt the interpretation that protects the integrity of the safe harbor instead of creating a loophole.

Part I applied such an approach in dissecting the relationship between vicarious liability and the DMCA safe harbors. Just as courts have already interpreted the DMCA's requirement of a “right and ability to control such [infringing] activity” more narrowly than the analogous requirement for vicarious liability, courts should also interpret the DMCA's requirement of “a financial benefit directly attributable to the infringing activity” as requiring greater attribution than the simple “direct financial benefit” requirement under the common law. Otherwise, the DMCA safe harbors would contain a gaping loophole for vicarious liability, leaving all Internet companies exposed to potentially limitless liability. Every single commercial Internet company on the Internet that deals with content of third parties—from AOL to Google to MySpace to Yahoo!—would be at serious risk of vicarious liability.

To their credit, an increasing number of courts have begun to apply this interpretive principle against loopholes in the DMCA. For example, the *Hendrickson v. eBay* court's narrow interpretation of “right and ability to control” was adopted to avoid “defeat[ing] the purpose of the DMCA and render[ing] the statute internally inconsistent.”¹⁴⁸ As the court recognized, “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.”¹⁴⁹

¹⁴⁸ *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1093 (C.D. Cal. 2001)

¹⁴⁹ *Id.* at 1093-94.

Likewise, in the recent video website case *UMG Recordings, Inc. v. Veoh Networks, Inc.*, the district court rejected a similar attempt to read § 512(c)'s safe harbor so narrowly that it would protect only an Internet company's mere storage of "material at the direction of the user," but *not* if anyone later accessed or displayed the stored material on the Internet.¹⁵⁰ Plaintiff Universal Music Group's interpretation, if adopted, would have rendered the § 512(c) safe harbor a complete nullity. Virtually all Internet companies that are in the business of hosting third-party content—ranging from website hosting companies such as Godaddy to content companies such as MySpace, Facebook, or YouTube—host third-party content so the content can be shared with others on the Internet.¹⁵¹ After all, the Internet is a huge network *for dissemination of content*.

In rejecting Universal Music's argument, Judge Matz adopted the reading of § 512(c) that would not eviscerate it. The text of § 512(c) says that "[a] service provider shall not be liable for monetary relief *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...."¹⁵² According to Matz, "by reason of" meant "as a result of" or "attributable to."¹⁵³ "So understood, when copyrighted content is displayed or distributed on Veoh it is 'as a result of' or 'attributable to' the fact that users uploaded the content to Veoh's servers to be accessed by other means."¹⁵⁴ Judge Matz fortified his textual analysis with several very persuasive passages rejecting Universal Music's loophole reading; for example, Matz reasoned:

If providing access could trigger liability without the possibility of DMCA immunity, service providers would be greatly deterred from performing their basic, vital and salutary function—namely, providing access to information and material for the public.¹⁵⁵

¹⁵⁰ *UMG Recordings, Inc. v. Veoh Networks, Inc.*, No. CV 07-5744 AHM, 2008 WL 5423841, at *7 (C.D. Cal. Dec. 29, 2008).

¹⁵¹ The one exception would be a web service (e.g., Dropbox, Box.net, or Mozy) that is in the business of private storage of material that is not necessarily ever shared with others on the Internet, such as to create backup files. See Mark Hendrickson, TechCrunch, *Dropbox: The Online Storage Solution We've Been Waiting For?*, March 11, 2008, at <http://www.techcrunch.com/2008/03/11/dropbox-the-online-storage-solution-weve-been-waiting-for/>. Such online storage services, although growing, are still relatively young and probably did not exist (at least not in any significant number) in 1998 when the DMCA was enacted. With the growth of "cloud" computing, in which data are stored remotely on servers through the Internet, this niche market can be expected to grow. See Lee, *supra* note 3, at 1500-01.

¹⁵² *UMG Recordings*, 2008 WL 5423841, at *5.

¹⁵³ *Id.* at *7.

¹⁵⁴ *Id.*

¹⁵⁵ *Id.* at *7; see also *id.* at *8 ("The 'safe harbor' would in fact be full of treacherous shoals if the copyright owner still could recover damages because the service provider remained liable for having provided access to the stored material that had been removed."); *id.* ("It is very difficult to see how the DMCA could achieve these goals if service providers otherwise eligible for limited liability under § 512(c) were exposed to liability for providing access to works stored at the direction of users. Such liability would surely undercut the 'robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age.'"); *id.* at 9 ("But as discussed above, this cooperative process would be pointless if service providers who provide access to material stored on their systems at the direction of users were precluded from limiting their potential liability merely because their services enabled users to access such works. The threat of such liability would create an enormous disincentive to provide access, thereby limiting the 'variety and quality of services on the Internet.'").

Judge Matz’s opinion is a perfect example of how to apply the principle against reading loopholes into the DMCA.

2. The need for certainty and clarity in the DMCA safe harbors

Second, the DMCA safe harbors should be interpreted or clarified in a way to promote certainty and clarity for private planning. Both the courts in construing the DMCA and Congress in possibly updating it should consider the need for certainty and clarity in the DMCA safe harbors in order for them to be at all effective. An uncertain or unclear “safe harbor” is self-defeating and of no practical use because it cannot guide people on how to act to avoid liability.¹⁵⁶ Even worse, an uncertain or unclear safe harbor can act as a “trap” for even the wary by dangling the false prospect of immunity from liability to businesses that invest millions of dollars based on the unclear law trying to follow what *appears* to be a safe harbor. As Judge Matz noted in the *UMG Recordings* case, “[t]he ‘safe harbor’ would in fact be full of *treacherous shoals*,”¹⁵⁷ defeating the whole purpose of a safe harbor.

Because so few cases involving the DMCA safe harbor are ever litigated, courts should be mindful in those cases of the need to articulate clearly the specific steps Internet service providers can take to fall within the safe harbor. Of course, the statute is supposed to set forth these requirements. By enacting a safe harbor, Congress hoped for clarity to foster investment in Internet services.¹⁵⁸

But clarity is easier said than done. To the extent the statutory requirements are ambiguous as applied to particular set of facts, courts should attempt to provide clear guidance to the public on how the requirements can be met, bearing in mind the presumption against creating loopholes.

Although the Supreme Court has yet to consider a case involving the DMCA safe harbors, it has provided an opinion in a different context, a Title VII employment case, that can serve as a model to follow. In *Burlington Indus., Inc. v. Ellerth*, the Court set forth a safe harbor or affirmative defense under Title VII for employers against vicarious liability: “The defense comprises two necessary elements: (a) that the employer exercised reasonable care to prevent and correct promptly any sexually harassing

¹⁵⁶ See Edward Lee, *Rules and Standards for Cyberspace*, 77 NOTRE DAME L. REV. 1275, 1314-16 (2002) (discussing how rules promote predictability and private planning); *id.* at 1348-56 (discussing rule approach to CDA safe harbor); see also Gideon Parchomovsky & Kevin A. Goldman, *Fair Use Harbors*, 93 VA. L. REV. 1483, 1502-03, 1510-11 (2007) (discussing benefits of crafting clear and certain safe harbor rules); *id.* at 1511 (“Consistent with the above observations, our proposed safe harbors seek to eliminate uncertainty wherever possible.”).

¹⁵⁷ *UMG Recordings, Inc. v. Veoh Networks, Inc.*, No. CV 07-5744 AHM, 2008 WL 5423841, at *8 (C.D. Cal. Dec. 29, 2008) (emphasis added).

¹⁵⁸ S. Rep. 105-190, at 8 (“without clarification of their liability, service providers may hesitate to make the necessary investment in the expansion and speed and capacity of the Internet”); *id.* at 20 (Title II “provides greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities”).

behavior, and (b) that the plaintiff employee unreasonably failed to take advantage of any preventive or corrective opportunities provided by the employer or to avoid harm otherwise.”¹⁵⁹ The Court elaborated:

While proof that an employer had promulgated an antiharassment policy with complaint procedure is not necessary in every instance as a matter of law, the need for a stated policy suitable to the employment circumstances may appropriately be addressed in any case when litigating the first element of the defense. And while proof that an employee failed to fulfill the corresponding obligation of reasonable care to avoid harm is not limited to showing any unreasonable failure to use any complaint procedure provided by the employer, a demonstration of such failure will normally suffice to satisfy the employer's burden under the second element of the defense. No affirmative defense is available, however, when the supervisor's harassment culminates in a tangible employment action, such as discharge, demotion, or undesirable reassignment.¹⁶⁰

The Court adopted this safe harbor for employers under Title VII “[i]n order to accommodate the agency principles of vicarious liability for harm caused by misuse of supervisory authority, as well as Title VII’s equally basic policies of *encouraging forethought* by employers and saving action by objecting employees.”¹⁶¹

Although Title VII’s regulation of the employment setting is pretty different from the DMCA’s regulation of Internet activities (and I do not want to stretch the analogy here),¹⁶² some of the general lessons already learned under Title VII are instructive for the more recently enacted DMCA. Like Title VII, the DMCA deals with difficult issues of secondary liability in contexts where primary or direct liability can be expected to recur. Both statutes attempt to *encourage forethought* and remedial action on part of those entities that can potentially face repeated lawsuits for secondary liability based on the conduct of others. Just as the *Ellerth* Court interpreted Title VII to establish a safe harbor for employers that set up and implement an antiharassment policy with complaint procedure for employees, the DMCA establishes a safe harbor for Internet service providers that reasonably implement a “repeat infringer” policy with a complaint procedure for notice-and-takedown.¹⁶³

¹⁵⁹ 524 U.S. 742, 765 (1998).

¹⁶⁰ *Id.*

¹⁶¹ *Id.* at 764 (emphasis added).

¹⁶² The *Ellerth* framework, as subsequently applied by lower courts, has generated a fair amount of criticism as being unduly stringent on employees in requiring unreasonable expectations of whether and how soon they complain to the employer about alleged harassment in the workplace. See Martha Chamallas, *Title VII’s Midlife Crisis: The Case of Constructive Discharge*, 77 S. CAL. L. REV. 307, 373 (2004). Obviously, an employee who is possibly subject to harassment stands in a much different and more precarious position than a copyright holder complaining about infringement. This suggests, however, that the DMCA’s placing the burden on copyright holders to report suspected infringement to ISPs is not too onerous. If employees who are subject to harassment can be expected to report harassment to employers even though such reporting may cause retaliation or other reprisals on the employee, copyright holders, who face no such risks or reprisal, can be expected to report infringement to ISPs under the DMCA notice and take-down procedure.

¹⁶³ 17 U.S.C. § 512(i) (repeat infringer policy); *id.* § 512(c)(1)(C) (notice and takedown); *id.* § 512(c)(2) (designated agent for DMCA notices).

3. The need for updating the DMCA

The relative lack of litigation over the DMCA safe harbors in the past 10 years suggests that Congress should itself periodically review the DMCA safe harbors, particularly as new web applications and technologies continue to develop at almost dizzying speed. Congress should consider granting the Librarian of Congress (or a designated agency) the rulemaking authority to establish new safe harbors for ISPs through administrative proceedings. Such a provision already exists in Title I of the DMCA granting the Librarian the power and the responsibility to recognize temporary exceptions to the anticircumvention provision.¹⁶⁴ The Title I provision *requires* the Librarian to consider, every three years, possible exceptions “upon the recommendation of the Register of Copyrights, who shall consult with the Assistant Secretary for Communications and Information of the Department of Commerce.”¹⁶⁵ This rulemaking process for exceptions was intended to accommodate “persons who are users of copyrighted work [who] are, or are likely to be in the succeeding 3-year period, adversely affected” by the anticircumvention provision.¹⁶⁶

My proposal has one key difference from Title I’s rulemaking procedure. Because entire Internet businesses can be constructed to meet the DMCA safe harbors, with millions of dollars invested, any future safe harbors recognized in the proposed rulemaking process should be permanent, not temporary. It would be unreasonable to expect an Internet company to expend millions of dollars to conduct a business that falls within a safe harbor, only to have that safe harbor disappear.

B. Principles for Making the Internet Work

The next set of principles relate to the fact that the DMCA safe harbors regulate the Internet, a speech technology. Amidst the all the statutory complexity, it may be easy to forget that the DMCA deals with the Internet. As Congress itself noted in committee reports, the statute should not be applied in way to retard the development of this network and revolutionary technology that has such considerable importance for First Amendment activities.¹⁶⁷ Efforts to combat copyright infringement must be balanced with the need to avoid restricting or retarding the Internet. Accordingly, where the text allows, courts should interpret the DMCA safe harbors in a way that avoids seriously undermining the Internet’s development. I offer two principles to serve that end.

1. Automated features and industry standards

First, courts should be wary of arguments that rely on imputing liability based on mere *automated* features of the Internet or websites, or features that have become industry wide standards or that enable interoperability. Copyright holders have routinely

¹⁶⁴ 17 U.S.C. § 1201(a)(1)(C).

¹⁶⁵ *Id.*

¹⁶⁶ *Id.*

¹⁶⁷ S. Rep. 105-190, at 1-2 (1998) (“to facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age”)

attempted to hold companies liable for mere *automated* systems that deal with third-party content or transmissions. Often, copyright holders seek to require Internet companies to engage in individual *human* review of content or links instead of using an automated system. As discussed above, the so-called “red flags” theory can easily devolve into such a request. Courts should be skeptical of these sorts of arguments.

Congress understood that the DMCA safe harbors were needed to protect Internet services from limitless liability that could be imposed on such services based simply on how the Internet must function to handle vast amounts of material throughout the network. As the Senate Report explained:

In the ordinary course of their operations service providers must engage in all kinds of acts that expose them to potential copyright infringement liability. For example, service providers must make innumerable electronic copies by simply transmitting information over the Internet. Certain electronic copies are made to speed up the delivery of information to users. Other providers engage in directing users to sites in response to inquiries by users or they volunteer sites that users may find attractive. Some of these sites might contain infringing material. In short, by 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.¹⁶⁸

Moreover, in the context of describing the safe harbor for passive conduits in subsection (a), the House Report indicated that automated processes should *not* be interpreted to disqualify an Internet service provider as a passive conduct, rejecting the theory that an automated process meant that the ISP was the one that actually “select[ed] ... the material” sent through its automated service by users.¹⁶⁹

Even before the DMCA was enacted, courts recognized serious problems with arguments against using automated features of the Internet. For example, Judge Whyte in *Netcom* rejected a claim of direct liability against a bulletin board operator that allowed third parties to post messages on its system.¹⁷⁰ Judge Whyte analogized Netcom’s “designing or implementing a system that automatically and uniformly creates temporary copies of all data sent through it” to the designing of “a copying machine [that] lets the public make copies with it.”¹⁷¹ The court rejected an interpretation of the Copyright Act that would make liable “every single Usenet server in the worldwide link of computers transmitting [the plaintiff’s] message to every other computer.”¹⁷² In order for direct liability to attach, the Copyright Act requires an act of copying of greater “volition” by defendant than merely setting up an automated system on the Internet.¹⁷³ In addition, Judge Whyte recognized the likely chilling of speech that could arise if Internet

¹⁶⁸ *Id.* at 8.

¹⁶⁹ H.R. Rep. 105-511(II), at 51.

¹⁷⁰ *Religious Tech. Ctr. v. Netcom Online Commcn. Serv., Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995).

¹⁷¹ *Id.* at 1369.

¹⁷² *Id.*

¹⁷³ *Id.* at 1370.

intermediaries had to prescreen by human inspection every piece of content or information posted by users.¹⁷⁴

The House Report to the DMCA endorsed the *Netcom* approach.¹⁷⁵ The wisdom of Judge Whyte's decision is that it recognizes that the Internet, which is a vast worldwide network of communication channels, depends on the ability to handle vast amounts of content in an *automated* system. No one "runs" the Internet. At least in free societies, no one prescreens who can post what. Thankfully, we do not have to wait for permission or human review to send an email or upload a photo.

Indeed, many of the most used and useful web applications on the Internet are offered to the public, often without charge, through *intermediaries*, or, in the terminology of the DMCA, Internet service providers. These intermediaries are able to service the huge demands of the public only because the intermediaries set up *automated* technological systems that can scale to enormous proportions. As Lemley aptly noted, "Internet intermediaries—service providers, Web hosting companies, Internet backbone providers, online marketplaces, and search engines—process hundreds of millions of data transfers every day, and host or link to literally tens of billions of items of third party content. They can process and host that data instantaneously only because they automate the process."¹⁷⁶ The danger in the copyright holders' argument against automated systems is that, if accepted, it would threaten to put intermediaries out of business, or to force them to dismantle their automated features that are so basic to Internet usage.

Take, for example, Universal Music's case against the video-sharing site Veoh. Universal argued that Veoh did not fall within the DMCA safe harbor for storing videos of its users because Veoh had set up an automated system that (i) converted each video into a common Flash file format to make them easier to watch on any video player and also (ii) "chunked" some of the videos into smaller chunks of the original file in order to make them more manageable.¹⁷⁷ Universal's theory was that the storage of the Flash-formatted files and the chunked files on Veoh's system was done "at the direction of" Veoh, and not Veoh's user as required to fall within the safe harbor.¹⁷⁸ In other words, even though the videos were originally uploaded onto Veoh's system at the direction of Veoh users, Universal argued that Veoh's automated conversion of those videos into an easier format and size to view on the Internet meant that the videos were no longer stored at the direction of the Veoh users, but were instead stored at the direction of Veoh (by means of its automated system).

Canvassing the case law, Judge Matz rejected Universal's argument. Judge Matz cited approvingly to *Io Group, Inc. v. Veoh Networks, Inc.*, in which the Northern District

¹⁷⁴ *Id.* at 1377-78 ("If Usenet servers were responsible for screening all messages coming through their systems, this could have a serious chilling effect on what some say may turn out to be the best public forum for free speech yet devised.").

¹⁷⁵ H.R. Rep. 105-511(I), at 24.

¹⁷⁶ Lemley, *supra* note 4, at 101.

¹⁷⁷ *UMG Recordings, Inc. v. Veoh Networks, Inc.*, No. CV 07-5744 AHM, 2008 WL 5423841, at *1 (C.D. Cal. Dec. 29, 2008).

¹⁷⁸ *Id.* at *6.

of California rejected the exact same argument about the automated conversion into Flash format of video files.¹⁷⁹ In *Io Group*, the district court noted that, unlike the definition of service providers that act as passive conduits for Internet transmissions under § 512(a),¹⁸⁰ the definition for service providers for the § 512(c) safe harbor did *not* contain a restriction that the service provider cannot modify the content of the user material.¹⁸¹ Moreover, Veoh's automated conversion process did not change the basic fact that the video file was uploaded by a user. Without the user, there would be no video on Veoh's system. "Veoh has simply established a system whereby software automatically processes user-submitted content and recasts it in a format that is readily accessible to its users."¹⁸² Agreeing with *Io Group*, the *UMG Recordings* court ruled that Veoh's automated conversion affected "only the form and not the content of the movies" uploaded by users.¹⁸³

Both of these decisions do a great job in attempting to interpret the DMCA safe harbors in a way that makes the Internet workable. As discussed above, automated systems are necessary for intermediaries to handle the unbelievable amounts of data and content that are transmitted over the Internet. Although not discussed in these two cases against Veoh, the vast majority of videos on the Internet are converted into Flash format, which today is the industry standard.¹⁸⁴ YouTube, the first company to solve the difficulty of watching videos online, chose the Flash format because it provided a universal format that could easily be played on most video players and also embedded on other sites, all while providing a more instantaneous viewing (without annoying lags in time for buffering).¹⁸⁵

Put more starkly, if Universal Music's argument were accepted, the *entire* online video sharing industry today would have to shut down. This is no exaggeration. Because YouTube and most other video sharing services (such as blip.tv, Dailymotion, Veoh, Yahoo!) use an automated system of Flash-formatted conversion of user-submitted videos, they would all fall outside the DMCA safe harbors under Universal Music's argument. In other words, all these companies would be exposed to massive copyright

¹⁷⁹ *Io Group, Inc. v. Veoh Networks, Inc.*, -- F. Supp. 2d --, 2008 WL 4065872 (N.D. Cal. Aug. 27, 2008).

¹⁸⁰ 17 U.S.C. § 512(k)(1)(A).

¹⁸¹ *Id.* § 512(k)(1)(B). See *Io Group*, 2008 WL 4065872, at *12-*13.

¹⁸² *Io Group*, 2008 WL 4065872, at *13.

¹⁸³ *Id.* at *10.

¹⁸⁴ See Flash Video Learning Guide, Adobe, http://www.adobe.com/devnet/flash/articles/video_guide.html ("Since the introduction of Flash video in 2002, Flash Player has become the most widely installed Internet video client, running on over 96% of all Internet-connected personal computers. Also, Flash Player runs on a wide variety of platforms and operating systems. The ubiquity of Flash Player ensures that most visitors can view Flash video without downloading additional plug-ins, so you can reach more people with lower development, testing, and support costs.").

¹⁸⁵ YouTube co-founder Steve Chen attributes the success of YouTube in solving the difficulty of sharing videos to choosing a single universal format that can be easily viewed and embedded. See *YouTube co-founder Steve Chen @ NewTeeVee Live*, Nov. 23, 2007, at <http://blip.tv/file/499719>; *Charlie Rose – Preview of Interview with YouTube Co-founders*, Aug. 9, 2006, at <http://www.youtube.com/watch?v=7E6E9q8Jebw>. For a general discussion of the Flash format and its benefits, see Jacqueline Emigh, *New Flash Player Rises in the Web-Video Market*, at <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=01597078>.

liability. If these companies chose to abandon the Flash format for videos, it would cripple the ability of people to share and watch videos online. Without Flash, the Internet would be back to the days before YouTube, circa 2004, when no one had solved the problem of how to allow everyone to upload and watch videos online.

The thought of returning the Internet to the state of 2004 should give any court serious pause. Flash-formatted videos are what allowed President Barack Obama and the other presidential candidates to reach millions of voters and others around the world through YouTube and other sites, all for free. By Election Day, Obama had 94.5 million views collectively of over 1,800 videos Obama posted on YouTube.¹⁸⁶ During the transition, Obama started to post videos of his weekly address on YouTube,¹⁸⁷ a practice that put the presidency (and the radio address) firmly into the Internet Age. For his Inauguration, Obama posted videos as well.¹⁸⁸ And, once in office, Pres. Obama opened up a White House channel on YouTube with videos from his presidency.¹⁸⁹ All of these videos are Flash-formatted. All were uploaded “at the direction of” Pres. Obama. YouTube and other video-sharing services should not lose their protection under the DMCA safe harbor just because they set up an automated system that enables any individual, from Pres. Obama to the person on the street, to share a video in a universal format that increases the potential audience of the video.

2. Freedom of the press and fostering technological innovation

Finally, there is the Free Press Clause. Elsewhere, I have written extensively about how the Framers understood the Free Press Clause as a direct limit on the Copyright Clause.¹⁹⁰ One of the core abuses that the Framers sought to end was the restriction of speech technologies, such as limits on the number and ownership of printing presses during 16th century England, as a way to protect copyrights.¹⁹¹ The Free Press Clause was meant to prohibit Congress from using copyright law to restrict speech technologies.¹⁹² Just as the Framers were wary of government depriving the people of arms, so too the Framers feared that government might deprive the people of the printing press.¹⁹³

To be faithful to the Free Press Clause, courts should interpret the DMCA safe harbor, where possible, in a way to avoid First Amendment problems.¹⁹⁴ Because the DMCA safe harbors regulate Internet services that facilitate the widescale dissemination

¹⁸⁶ See Edward Lee, *Analyzing the Presidential Candidates’ Videos on YouTube* (manuscript).

¹⁸⁷ See ChangeDotGov YouTube channel, <http://www.youtube.com/user/ChangeDotGov>.

¹⁸⁸ See Inauguration YouTube channel, <http://www.youtube.com/user/inauguration?blend=1>.

¹⁸⁹ See White House YouTube channel, <http://www.youtube.com/user/whitehouse>.

¹⁹⁰ See Edward Lee, *Guns and Speech Technologies: How the Right to Bear Arms Affects Copyright Regulations of Speech Technologies*, 17 WM. & MARY BILL RTS. J. (forthcoming May 2009); *Freedom of the Press 2.0*, 42 GEORGIA L. REV. 309 (2008).

¹⁹¹ See Lee, *Guns and Speech Technologies*, *supra* note 190; Lee, *Freedom of the Press 2.0*, *supra* note 190, at 330-56.

¹⁹² See Lee, *Freedom of the Press 2.0*, *supra* note 190.

¹⁹³ See Lee, *Guns and Speech Technologies*, *supra* note 190.

¹⁹⁴ See generally *Salinas v. U.S.* 52, 59-60 (1997) (canon of constitutional doubt).

of speech by the public, courts must avoid letting copyright law restrict or prohibit speech technologies. In addition, because the DMCA safe harbors operate as First Amendment safeguards within copyright law—promoting the development of speech technologies on the Internet—“it is appropriate to construe copyright’s internal safeguards to accommodate First Amendment concerns.”¹⁹⁵

For far too long, courts and commentators have ignored this core protection of the Free Press Clause.¹⁹⁶ In the past, this oversight was perhaps understandable, given that the traditional contours of copyright law dating back to the First Copyright Act did not ever attempt to regulate speech technologies.¹⁹⁷ But that all changed beginning in the late 20th century when copyright holders sought to hold technology developers liable based on the conduct of users of their technology. In 1984, the Supreme Court established the *Sony* safe harbor that provides technology developers immunity from liability for developing a technology that is “capable of substantial noninfringing uses.”¹⁹⁸ In *Sony*, the Court held that Sony, the developer of the betamax or video recorder, could not be held liable for making a technology that was capable of copying for fair use purposes.¹⁹⁹ In prior scholarship, I have argued that the *Sony* safe harbor operates as a traditional First Amendment safeguard²⁰⁰ within copyright law to serve Free Press interests and the development of speech technologies.²⁰¹

For similar reasons, the DMCA safe harbors act as important First Amendment safeguards within copyright law for the Internet. There can be no doubt that the Internet receives full First Amendment protection.²⁰² Indeed, the Supreme Court made special note of how the amazing functions and technologies of the Internet can enable any person to be a publisher to a potential audience of millions.²⁰³ As the Court put it in 1997, “[t]his dynamic, multifaceted category of communication includes not only traditional print and news services, but also audio, video, and still images, as well as interactive, real-time dialogue.”²⁰⁴ The DMCA was enacted to foster the development of these revolutionary technologies, and to “ensure[] that the efficiency of the Internet will

¹⁹⁵ Eldred v. Ashcroft, 537 U.S. 186, 221 n.24 (2003).

¹⁹⁶ It is noteworthy that Congress, in DMCA anticircumvention provision, expressly recognized the need not to allow that provision to infringe the freedom of the press. 17 U.S.C. § 1201(c)(4) (“Nothing in this section shall enlarge or diminish any rights of free speech or free press for activities using consumer electronics, telecommunications, or computing products.”).

¹⁹⁷ See Lee, *Freedom of the Press 2.0*, *supra* note 185, at 351-54.

¹⁹⁸ Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984).

¹⁹⁹ *Id.*

²⁰⁰ “First Amendment safeguard” within copyright is a term of art recognized by the Supreme Court. See Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 556 (1985); Eldred v. Ashcroft, 537 U.S. 186, 221 (2003). Thus far, the Court has identified two such safeguards, the fair use doctrine and the idea-expression dichotomy. *Harper & Row*, 471 U.S. at 560. First Amendment safeguards within copyright law operate to keep copyright law from violating legitimate First Amendment activity. Because of these safeguards, the typical copyright case does not require First Amendment scrutiny. *Eldred*, 537 U.S. at 221.

²⁰¹ See Lee, *Freedom of the Press 2.0*, *supra* note 190, at 373.

²⁰² Reno v. American Civil Liberties Union, 521 U.S. 844, 870 (1997).

²⁰³ *Id.* at 853, 870.

²⁰⁴ *Id.* at 870.

continue to improve and that the variety and quality of services on the Internet will expand.”²⁰⁵

The DMCA safe harbors thus provide an important First Amendment safeguard for web technologies. Although copyright law can proscribe infringement on the Internet, copyright law cannot prohibit Internet technologies that are capable of substantial noninfringing uses under the *Sony* safe harbor.²⁰⁶ The DMCA safe harbors provide an additional layer of regulation and immunity for Internet services that have ongoing relationships with their users. These services are required to help in reducing the infringement of their users by adopting repeat infringer policies and notice-and-takedown procedures under the DMCA.²⁰⁷ If they do, the DMCA safe harbors offer the web services immunity from copyright liability. In the end, such protection fosters the development of speech technologies on the Internet, which in turn fosters the creation and sharing of speech by millions of people around the world.

Conclusion

The DMCA is a decade old, which, in Internet time, may well be closer to a century. Although the DMCA safe harbors have helped to foster tremendous growth in web applications, several very basic aspects of the DMCA safe harbors remain uncertain. This Essay has attempted to clear up two of the biggest uncertainties regarding the DMCA’s relationship to vicarious liability, and the so-called “red flags” theory. Of course, it is up to the courts and Congress to provide the necessary clarity to these and other issues in the future. This Essay offers five principles for courts and Congress to consider in applying or amending the DMCA safe harbors in the future. The DMCA safe harbors should be made truly “safe” harbors, in a way that encourages greater investment in and the development of speech technologies on the Internet.

²⁰⁵ S. Rep. 105-190, at 2.

²⁰⁶ *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 442 (1984).

²⁰⁷ See 17 U.S.C. § 512(c), (i).