

**CATCHING THE CONSCIENCE: AN
ANALYSIS OF THE KNOWLEDGE THEORY
UNDER § 512(C)'S SAFE HARBOR & THE
ROLE OF WILLFUL BLINDNESS IN THE
FINDING OF RED FLAGS**

*Methaya Sirichit**

ABSTRACT

The application and interpretation of § 512(c)'s safe harbor of the Digital Millennium Copyright Act (DMCA) has been regarded as a notoriously inexact science that provides a confounding experience to both legal practitioners and judges. Much of the disagreement is based on the fact that the DMCA was passed in 1998 as a compromised regime of limitation to copyright liability for online providers, based on notice-and-takedown procedures, whereas the common-law jurisprudence of secondary liability keeps expanding as technologies continue to evolve. The result is a stark contrast between the knowledge theory that determines safe-harbor eligibility of a service provider and the one that determines whether a cognitive element under contributory liability doctrine has been met. On one hand, the incongruence between these two cognitive theories has threatened the integrity of the DMCA's safe harbors. On the other hand, courts have been unable to provide any useful guidance for a practical application of a "red flag" test – a tool designed by Congress to combat online piracy and to distinguish responsible service providers from cynical ones.

This paper suggests that, for the safe harbor to achieve its central purposes, future interpretations of the § 512(c) must be

* LL.B., Thammasat University Thailand, 2000; LL.M., (International Commercial Law), University of Kent at Canterbury (UK), 2003; LL.M. (Intellectual Property), George Washington University Law School, 2005; S.J.D. candidate, George Washington University Law School. Member, Thai Bar Association; lecturer of Intellectual Property Law, Naresuan University.

undertaken under the principle that the knowledge elements of the DMCA are inherently non-coextensive with that of contributory liability doctrine. The paper argues that courts' repeated failures to demonstrate how the red flag test can be concretely applied have led to a now predominant reliance on the willful blindness doctrine in establishing apparent knowledge. The Ninth Circuit's recent decision, *UMG Recording, Inc. v. Shelter Capital Partner LLC*, managed, to some extent, to reduce ambiguities that have long plagued judicial determinations of the red flag test and re-attuned it to the underlying structure of § 512(c). However, it is suggested that Congress initiate a public-participation program for the purpose of revising the means through which "apparent knowledge" could be demonstrated while preserving the integrity of the DMCA's notice-and-takedown safe harbor.

TABLE OF CONTENTS

ABSTRACT	85
TABLE OF CONTENTS	86
I. INTRODUCTION	88
II. THE CONTOURS OF SECONDARY COPYRIGHT LIABILITY	94
A. Common Law Secondary Liability.....	94
1. Contributory Liability.....	94
2. Vicarious Liability	95
B. Knowledge Theory under the Common Law Secondary Liability	97
1. The Traditional Application and Recent Changes.....	97
2. Sony Doctrine and the Limit on Imputing Requisite Knowledge	100
3. The Ninth Circuit's Interpretation of <i>Sony</i> Doctrine in <i>Napster</i>	105
4. <i>In re Aimster</i> and Doctrine of Willful Blindness ..	105
5. <i>Grokster</i> and Copyright Inducement Liability	112
III. SAFE HARBORS UNDER THE DIGITAL MILLENNIUM COPYRIGHT ACT	117
A. Purpose & Background	117
B. General Contour of the DMCA Safe Harbor	118
1. Threshold Requirements	119
a. Repeat Infringer Termination Policy (R.I.P.) ..	119
b. Standard Technical Measures	122

2013]	SAFE HARBOR & WILLFUL BLINDNESS	87
	2. Statutory Notice-and-Takedown Safe Harbors	123
IV.	KNOWLEDGE STANDARD UNDER NOTICE & TAKE DOWN SYSTEM OF § 512(C).....	124
	A. Independent Knowledge Standard of the DMCA.....	125
	B. Notice-Centrality Aspect of Actual Knowledge	128
	C. Apparent Knowledge or “Red Flag” Test.....	132
	1. The Inherent Paradoxes of the Red Flag Test	133
	a. Apparent Knowledge and Reasonable Person Standard.....	133
	b. Proving Red Flag Appears to Be an Insurmountable Task.....	135
	i. General Judicial Disregard of Legislative Recommendation	136
	ii. Unavailability of Other Evidence	139
	iii. The Causes of Judicial Reluctance in Finding Red Flag Knowledge and the Legal Tension it Creates	142
	2. Red Flag Test and “Willful Blindness” Doctrine...	145
	a. Courts’ Receptiveness toward “Willful Blindness” Argument	145
	3. The Impact of Supreme Court’s Formulation of Willful Blindness in Global Tech Appliances	148
	a. Willful Blindness and “Copyright Thief” Discourse	150
	b. The DMCA and Inducement Liability	155
V.	THE NINTH CIRCUIT’S INTERPRETATION OF THE DMCA’S KNOWLEDGE STANDARD IN THE UMG-VEOH DISPUTE	156
	A. Overview	156
	B. Background of the UMG-Veoh Dispute	158
	C. The Ninth Circuit’s UMG III Decision	162
	1. UMG’s Arguments	163
	a. UMG’s Argument on Actual Knowledge.....	163
	b. UMG’s Argument on Apparent Knowledge	165
	c. UMG’s Argument on Willful Blindness	166
	2. The Ninth Circuit’s Decision	168
	a. Rejecting UMG’s “general awareness” theory.	169
	b. Apparent Knowledge or Red Flag.....	171
	c. Willful Blindness and “the Right and Ability to Control”	174
	d. The DMCA Requirements and Elements under Common Law Secondary Liability Are Not Coextensive	175

3. Case Analysis.....	177
a. Actual Knowledge Means Knowledge of <i>Actual</i> Infringement.....	177
b. “Red Flag” is Still a Meaningful Test for DMCA–Eligibility Determination.....	179
c. Interpretation of DMCA’s Requirements Is To Be Made Independently of Common Law Secondary Liability Jurisprudence.....	182
VI. SUGGESTIONS & RECOMMENDATIONS.....	185
VII. CONCLUSION	189

I. INTRODUCTION

Knowledge is almost always a prerequisite component of action. All of us need certain information before we can properly act in a given circumstance. In William Shakespeare’s foremost play, *The Tragedy of Hamlet*, the protagonist was constantly plagued throughout the play with uncertainty regarding the death of his father, King Hamlet.¹ The Prince of Denmark suspected that his uncle, now King Claudius, was a usurper of the throne.² But how did Hamlet become convinced of his uncle’s foul deed? He talked to a ghost.³ The Ghost, who claimed to be the spirit of Hamlet’s murdered father, divulged the truth to the Prince and prompted him to revenge.⁴ Hamlet took steps to investigate.⁵ Rather than seeking concrete evidence, however, Hamlet devised a play—*the Mouse-trap*—through which he hoped to “catch the conscience of the king” during a performance.⁶ *The Mouse-trap* worked like a dream, yet Hamlet did not act.⁷ The rest, as we know, is a tragedy.⁸ It is often said that had Hamlet not listened to the Ghost, a lot of lives in the play would have been saved, including his own.⁹ Other critics

¹ William Shakespeare, *The Tragedy of Hamlet, Prince of Denmark* act 1, sc. 2.

² *Id.*

³ *Id.* at act 1, sc. 5.

⁴ *Id.*

⁵ *Id.*

⁶ SHAKESPEARE, *supra* note 1, at act 2, sc. 2.

⁷ *Id.* at act 3, scs. 2, 3 (“Up sword; and know thou a more horrid hent . . . This physic but prolongs thy sickly days.”).

⁸ *Hamlet Genre*, SHMOOP UNIV., INC., (Nov. 11, 2008), <http://www.shmoop.com/hamlet/genre.html>.

⁹ See Amanda Mabillard, *Revenge in Hamlet*, SHAKESPEARE-ONLINE.COM,

argued that Hamlet's downfall was on account of his own failure to act.¹⁰

Back to our non-theatrical world, online service providers (OSPs) are constantly mired in a similar dilemma of *to act or not to act*, when they come across knowledge or awareness of infringement.¹¹ Section 512(c) of the DMCA provides safe harbors for online providers whose operations—providing storage of information at direction of users—render them susceptible against claims of indirect infringement.¹² However, even though the DMCA operates in accordance with specific types of information, both the text of § 512(c) and its legislative history do not adequately clarify the appropriate knowledge standard for determining OSPs' eligibility for the safe harbors.¹³ To further complicate the matter, many of DMCA's requirements are worded similar to the elements of the common law secondary liability doctrine.¹⁴ This raises the question of whether the DMCA is actually designed to shield service providers from indirect copyright liability.¹⁵ Indeed, a plain reading of the text of § 512(c) suggest that an OSP necessarily forfeits its DMCA safe harbor as soon as it is found to be vicariously or contributorily

<http://www.shakespeare-online.com/playanalysis/revengetragedy.html> (describing how the ghost helped prompt the revenge plot) (last updated Dec. 3, 2011).

¹⁰ *Hamlet Essay*, ST. ROSEMARY EDUC. INST. (2012), <http://schoolworkhelper.net/hamlet-essay> (“[Hamlet’s] over thinking of the world around him is a reason for his indecisiveness and consequently his downfall.”).

¹¹ See *1999 Guidelines for Compliance with the Online Service Provider Provisions of the DMCA*, UNIV. OF CAL. (1999), <http://copyright.universityofcalifornia.edu/systemwide/pdmca.html> (discussing the need to approach instances of infringement “on a case-by-case” basis”).

¹² 17 U.S.C.A. § 512(c) (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/07/12).

¹³ See Mitchell Zimmerman, *Copyright Alert: Viacom v. YouTube/Google Second Circuit Reinstates Viacom’s Copyright Lawsuit, But Largely Affirms Pro-Online Service Provider Holdings*, FENWICK & WEST LLP (2012), http://www.fenwick.com/FenwickDocuments/Copyright_Alert_04-05-2012.pdf (discussing the knowledge standard for eligibility for the safe harbor provisions of the DMCA, as applied by the federal court system).

¹⁴ Veronica Corsaro, *From Betamax to YouTube: How Sony Corp. of America v. Universal City Studios, Inc. Could Still Be a Standard for New Tech.*, 64 FED. COMM. L.J. 449, 465 (2012).

¹⁵ See Jonathan J. Darrow & Gerald R. Ferrera, *Social Networking Websites and the DMCA: A Safe-Harbor from Copyright Infringement Liability or the Perfect Storm?*, 6 NW. J. TECH. & INTELL. PROP. 1, 7–8 (2007) (discussing secondary copyright liability and the DMCA).

liable under the common law.¹⁶ Taken together, these ambiguities do not only frustrate operations of certain online providers, who must deal with third-party copyrighted content on their systems,¹⁷ they also undermine the effectiveness of the safe harbor as a whole.¹⁸

Meanwhile, DMCA-qualifying OSPs continue to be disturbed by apparition-like information of infringement as well as copyright's version of *the Mouse-trap*.¹⁹ Copyright holders remain adamant in their belief that DMCA-compliant notices are not the only means to generate a level of awareness sufficient to compel an OSP to act, at the penalty of losing its safe harbor.²⁰ In their view, indicators of direct infringement can be found everywhere, and Congress—by incorporating the “red flag” test into the § 512(c)—clearly did not intend to exclude them from the eligibility calculus of the DMCA.²¹ On the contrary, right holders argue that OSPs should respond to other evidence—no matter how flighty or indirect—if it imparts enough information to create “general awareness” that some third-party infringement is at hand.²² They also emphasize that the DMCA does not seek to

¹⁶ Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. TELECOMM. & HIGH TECH. L. 101, 104 & n.23 (2007) (suggesting that § 512(c) may not provide protection against vicarious liability claims); R. Anthony Reese, *The Relationship Between the ISP Safe Harbors and the Ordinary Rules of Copyright Liability*, 32 COLUM. J.L. & ARTS 427, 438 (2009) (arguing that the DMCA only partially protects OSPs against contributory liability claims).

¹⁷ See Kuruvilla J. Olaso, *Two Conflicting Approaches to § 512(C): IO v. Veoh and UMG v. Veoh*, 25 BERKELEY TECH. L.J. 347, 355 (2010) (discussing the ambiguity in the safe harbor provisions of the DMCA).

¹⁸ See Lemley, *supra* note 16, at 104–05. “The overall effect is a set of ‘safe harbors’ that provides something less than perfect security for intermediaries . . .”

¹⁹ See *Corbis Corp., v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1109 (W.D. Wash. 2004) (stating that plaintiff's lacked evidence of blatant infringement to motivate defendant's to examine the information or act as a red flag for Defendants); SHAKESPEARE, *supra* note 1, at act 3, sc. 2.

²⁰ See Brief for Appellant at 50–53 *UMG Recordings, Inc. v. Shelter Capital Partners LLC (UMG III)*, 667 F.3d 1022 (9th Cir. 2011) (No. 09–56777), 2010 WL 3706518 [hereinafter *UMG's Opening Brief*] (arguing that the District Court eviscerated the originally intended effectiveness of the “red flag”); see also 17 U.S.C.A. § 512(c) (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/07/12) (establishing the “red flag” test).

²¹ *UMG's Opening Brief*, *supra* note 20, at 53; see also *Corbis Corp.*, 351 F. Supp. 2d at 1107 (discussing evidence proffered by plaintiffs to demonstrate awareness of infringement).

²² See *UMG III*, 667 F.3d at 1039–40 (demonstrating that Plaintiff argued for the use of a general awareness standard); *Io Grp., Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1148–49 (N.D. Cal. 2008) (arguing that general

shield an OSP who views such information with a straight face and is not prepared to act.²³ Failure to respond to certain categories of notice may indicate a service provider's ill conscience and willful ignorance.²⁴

Despite their repeated failures to persuade courts to adopt their arguments, the content industries' points as they relate to knowledge requirements, are not completely without merit.²⁵ Continued judicial rejections of red flag claims have conjured up doubts as to whether the apparent knowledge requirement under § 512(c)(1)(A)(ii) could ever be applied.²⁶ Common sense tells us that any interpretation that, in effect, expunges a passage out of a statute cannot be held truly satisfactory.²⁷ Indeed, red flag or apparent knowledge is a part of the balance that Congress struck when it enacted the DMCA.²⁸ Unfortunately, as DMCA jurisprudence implicitly suggests, the red flag test appears to be antithetical to the very tenet of the DMCA as a primarily notice-oriented safe harbor regime.²⁹ To make matters worse, the

awareness should compel action); *Corbis Corp.*, 351 F. Supp. 2d at 1108 (attempting to argue that Defendant had sufficient general awareness); *Capitol Records, Inc., v. MP3tunes, LLC (Capitol Records)*, 821 F. Supp. 2d 627, 644 (S.D.N.Y. 2011) (noting evidence offered by Plaintiffs to support their theory that Defendant's had an awareness of infringement).

²³ See *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93, 109 (2d Cir. 2010) (arguing that if a defendant is not legally responsible to ensure that users are not engaging in copyright infringement within its online domain it places an unreasonable burden on a plaintiff to ensure infringement is not occurring).

²⁴ See *Capitol Records*, 821 F. Supp. 2d at 637–38 (arguing that defendant purposefully blinded itself to user infringement); *Corbis Corp.*, 351 F. Supp. 2d at 1098 (stating that a service providers must remove infringing material upon notification or the provider itself will be exposed to copyright liability).

²⁵ See David Ludwig, *Shooting the Messenger: ISP Liability for Contributory Copyright Infringement*, 2006 B.C. INTELL. PROP. & TECH. F. 110701 (2006) (explaining the development of the constructive knowledge doctrine at the federal court level).

²⁶ See *Io Grp.*, 586 F. Supp. 2d at 1149 (holding that the “red flag” test was not satisfied); *Corbis Corp.*, 351 F. Supp. 2d at 1108–09 (indicating that purported evidence of alleged red flags was insufficient).

²⁷ *But cf. Viacom Int'l v. YouTube, Inc. (Viacom II)*, 676 F.3d 19, 31 (2d Cir. 2012) (discussing the court's interpretation of the “red flag” provision and their refusal to read out specificity requirements as requested by the Plaintiffs).

²⁸ See S. REP. NO. 105–190, at 49 (1998) (explaining Congressional rationale behind the “red flag” test).

²⁹ Courts are often unwilling to consider or accept arguments based on the “red flag test,” despite its presence in the statute. *Compare* 17 U.S.C.A. § 512(c) (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/07/12), *with Capitol Records*, 821 F. Supp. 2d at 627, 644–45 (denying plaintiff's suggestion that certain terms should be construed as “red flags”); *see also Io Grp.*, 586 F. Supp. 2d at 1149 (holding that the “red flag” test

legislative history does not seem to provide more than an obscure and not-so-well-contemplated guideline about how courts should apply the red flag test.³⁰ Thus, a practical determination of when the red flag test can be triggered continues to be an important goal for future interpretation of the DMCA.³¹

This paper seeks to systematically analyze the knowledge standard of the DMCA § 512(c) by comparing it with the knowledge theory under the secondary copyright liability doctrine. There are two central hypotheses in this paper. The first hypothesis is that the standard of knowledge under the DMCA is not parallel to that of common law contributory infringement.³² The DMCA, as a notice-centrality safe harbor regime, needs an independent knowledge standard to preserve the integrity of its notice protocol.³³ It is argued that, unless this hypothesis is true, the DMCA's general purpose—that § 512(c) provides effective safe harbor to service providers storing content at the direction of third party—will ultimately crumble.³⁴ The second hypothesis, on the other hand, provides rebutting evidence to the myth that courts conclusively ruled out the possibility of finding red flag awareness under the DMCA.³⁵ This paper seeks to show that courts, in fact, found apparent knowledge, based on the red flag test, in a number of cases—especially, whenever a plaintiff was able to prove that a defendant's conduct constituted willful ignorance of the facts regarding infringing circumstances.³⁶ Nonetheless, this study

was inapplicable); *Corbis Corp.*, 351 F. Supp. 2d at 1109 (indicating that purported evidence of alleged red flags was insufficient).

³⁰ See 17 U.S.C. § 512(c) (establishing the “red flag” test); see also S. REP. No. 105–190, at 49 (failing to lay out guidelines for the application of the “red flag” test).

³¹ See Liliana Chang, Note, *The Red Flag Test for Apparent Knowledge Under the DMCA § 512(c) Safe Harbor*, 28 CARDOZO ARTS & ENT. L.J. 195, 219–22 (2010) (discussing implications of judicial decisions on the red flag test and necessity of a standard in interpreting its application).

³² See *infra* Part II.B.

³³ See *infra* Part IV.A–B.

³⁴ See *infra* notes 253–266 and accompanying text; Part IV.B.

³⁵ See *Viacom II*, 676 F.3d 19, 31–32 (2d Cir. 2012) (stating that the actual knowledge provision does not eliminate the possibility of finding red flag knowledge, which can be applied to specific instances of infringement).

³⁶ See *Flava Works, Inc. v. Gunter*, No. 10 C 6517, 2011 WL 3205399, at *7–8 (N.D. Ill. July 27, 2011) (finding defendant's policy of only removing links/embeds not available on external websites “the epitome of ‘willful blindness’ and evidence of copyright infringement); *Columbia Pictures Indus. v. Fung*, No. CV 06-5578 SVW(JCx), 2009 WL 6355911, at *17–18 (C.D. Cal.

contends that while the doctrine of willful blindness is generally regarded as high bar,³⁷ it complicates a determination of an OSP's qualification for § 512(c)'s safe harbor because it shifts the focus from adequacy of evidence to an inquiry about an OSP's conscience and willingness to enforce copyright.³⁸ As a consequence, my study endorses the approach adopted by the Ninth Circuit in *UMG Recordings, Inc. v. Shelter Capital Partners, LLC (UMG III)*³⁹—seeking to clarify type(s) of evidence that can trigger apparent awareness of infringement without disturbing the notice-centrality aspect of the DMCA.⁴⁰ This practical approach would allow courts to apply “specific knowledge of particular infring[ement]” to the red flag test without resulting in the conflating the actual knowledge and the red flag awareness test together.⁴¹

This paper is divided in to six parts. In Part II, the knowledge standard under contemporary contributory liability jurisprudence will be analyzed along with other related doctrines, namely willful blindness and inducement. Part III will explain the general contours and basics of the DMCA, and Part IV will analyze and discuss the knowledge standard under § 512(c) of the DMCA on the basis of legislative history, recent case law interpreting § 512(c) and textual structure of the safe harbor itself.

Next, in Part V, the Ninth Circuit's latest interpretation of the DMCA in *UMG III* will be examined and discussed. The analysis of this case will be made in the light of conclusions and

Dec. 21, 2009) (determining sufficient evidence existed to establish defendants' awareness of red flags which indicated defendants willful blindness in avoiding knowledge of their users' infringement).

³⁷ See *Global-Tech Appliances v. SEB S.A. (Global-Tech Appliances)*, 131 S. Ct. 2060, 2070–71 (2011) (embracing two requirements of the willful blindness doctrine agreed upon by the Courts of Appeals and holding that a defendant “can almost be said to have actually known the critical facts,” thereby increasing the doctrine's stringency); see also *infra* Part II.B.4 at fns. 140–56 and accompanying text (discussing the Supreme Court's interpretation of the requirements under the willful blindness doctrine in *Global-Tech Appliances*).

³⁸ See *In re Aimster Copyright Litig. (In re Aimster)*, 334 F.3d 643, 655 (7th Cir. 2003) (“[Aimster's] ostrich—like refusal to discover the extent to which its system was being used to infringe copyright is merely another piece of evidence . . .”).

³⁹ *UMG III*, 667 F.3d 1022 (9th Cir. 2011).

⁴⁰ See *id.* at 1040 (stating email notification of infringement from a third party rather than a copyright holder may constitute apparent awareness because copyright holders are subject to statutory notification requirements).

⁴¹ *Id.* at 1037.

conceptual frameworks developed in the paper's previous sections. The scope of the discussion, however, will be largely confined to issues of knowledge, which is the focus of our study. Finally, in Part VI, this study shall communicate a number of suggestions and recommendations, which is hoped to provide more clarity to future application of § 512(c).

II. THE CONTOURS OF SECONDARY COPYRIGHT LIABILITY

A. *Common Law Secondary Liability*

The doctrine of secondary liability in American copyright law is largely based on invention of the courts and it is still evolving as we speak.⁴² Thus, although the copyright act does not say anything explicitly about liability of indirect infringers, "courts have long recognized that in certain circumstances, vicarious or contributory liability will be imposed" on a non-direct infringer.⁴³ The equitable consideration of fairness has led courts to adopt both the doctrine of vicarious liability and contributory infringement for the purpose of enforcing copyright against a defendant who did not directly violate the exclusive rights of the copyright holder, but rather contributed to the infringing conduct, or "whose economic rights [are] intertwined with the direct infringer's . . ." ⁴⁴

1. Contributory Liability

The concept of contributory liability stems from the tort law "notion that one who directly contributes to another's infringement should be held accountable."⁴⁵ It is "an outgrowth of . . . enterprise liability" which addresses the causational problem of identifying the circumstances where it is proper to spread the accountability of the direct infringer to other individuals.⁴⁶ A non-direct infringer will be contributorily liable

⁴² See *Metro-Goldwyn-Mayer Studios v. Grokster, Ltd. (Grokster I)*, 545 U.S. 913, 930 (2005) ("[T]hese doctrines of secondary liability emerged from common law principles . . .").

⁴³ *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 261 (9th Cir. 1996).

⁴⁴ *Id.* at 262.

⁴⁵ *Id.* at 264.

⁴⁶ *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 435–36 (1984), *superseded by statute*, Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended at 17 U.S.C.A. § 1201); 1 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12.04[A][3]

for a third party's conduct upon demonstration of two elements: (1) knowledge of direct infringement, which can be either actual or constructive knowledge,⁴⁷ and (2) acts of inducing, causing, or materially contributing to infringing activities.⁴⁸

2. Vicarious Liability

“The concept of vicarious . . . liability was . . . an outgrowth of the agency principles of *respondeat superior*.”⁴⁹ Courts overseeing copyright disputes, however, recognize that vicarious liability can extend beyond the scope of employment relationship.⁵⁰ Thus, “even in the absence of an employer—employee relationship one may be vicariously liable if he has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities.”⁵¹ However, the agency origin of the doctrine suggests that knowledge or awareness of an illegal act needs not be established to support this type of liability. Therefore, courts can “impose[] [vicarious] liability even though the defendant was unaware of the infringement.”⁵²

It is interesting that the absence of the knowledge prong of vicarious liability does not render all subjective or internal factors completely irrelevant. In early decisions such as *Shapiro, Bernstein & Co. v. H. L. Green Co.*, vicarious liability was found based on direct financial benefit coming *directly* from the sale of bootleg recordings made by the direct infringers.⁵³ The close relationship between the defendant store owner and the concessionaire in that case was close enough for the court to determine that there could be vicarious liability without awareness of the infringement.⁵⁴ However, subsequent courts have expanded the direct financial benefit prong to cover circumstances where an alleged indirect infringer demonstrates motive to profit—even though none of the financial benefit to

(Matthew Bender & Co., Inc. ed., 2012).

⁴⁷ *Ellison v. Robertson*, 357 F.3d 1072, 1076 (9th Cir. 2004).

⁴⁸ *Gershwin Publ'g v. Columbia Artists Mgmt.*, 443 F.2d 1159, 1162 (2d Cir. 1971).

⁴⁹ *Fonovisa*, 76 F.3d at 261–62 (emphasis added).

⁵⁰ *Gershwin*, 443 F.2d at 1162.

⁵¹ *Id.*

⁵² *Fonovisa*, 76 F.3d at 262.

⁵³ *Shapiro, Bernstein & Co. v. H. L. Green Co.*, 316 F.2d 304, 308 (2d Cir. 1963).

⁵⁴ *Id.*

such a party comes directly from the direct infringer.⁵⁵

Recent technological developments have caused profound effects on the application of vicariously liability. Modern peer-to-peer (P2P) communication protocol enabled technological providers to adopt a completely decentralized design that threatens to render the “right and ability to control” prong meaningless.⁵⁶ However, innovations in P2P architecture constitute only a small part of the big picture. The explosion of web 2.0 applications and modern cloud-based online services has forever changed the way people store and access their information. Most Internet users now rely on remotely stored and accessible contents more than what they actually keep on their system.⁵⁷ Therefore, a typical online “storage provider” has to deal with a prodigious amount of information entering through and residing on its servers on an everyday basis. Such operations raise innumerable questions regarding potential copyright liability.⁵⁸

More specifically, because these providers normally retain authority to suspend or even terminate the service to any user—a necessary strategy to keep their sites free of illegal or contraband materials—they are practically in control of myriads of content the existence of which they do not even know. Needless

⁵⁵ In *Fonovisa*, the defendant swap-meet operator only received venue-access fees from direct infringers. However, the court found that these revenues—including admission and parking fees—must be considered direct financial benefit if they were generated by the drawing power of infringing activities. *Fonovisa*, 76 F.3d at 263–64; see also, *A&M Records, Inc. v. Napster, Inc. (Napster II)*, 239 F.3d 1004, 1023 (9th Cir. 2001) (affirming the District Court’s holding that direct financial benefit does not require earned revenue so long as the defendant has economic incentives for tolerating unlawful behavior).

⁵⁶ Before the Supreme Court introduced “inducement liability” into the copyright law, the Court of Appeals of the Ninth Circuit had held that a completely decentralized architecture of the defendant *Grokster* rendered the plaintiff’s vicarious liability claim moot. *Metro-Goldwyn-Meyer Studios v. Grokster Ltd. (Grokster II)*, 380 F.3d 1154, 1165–66 (9th Cir. 2004), *vacated and remanded by* 545 U.S. 913 (2005).

⁵⁷ See JONATHAN L. ZITTRAIN, *THE FUTURE OF INTERNET AND HOW TO STOP IT* 185 (2008) (“[T]he use of our PCs is shrinking to that of mere workstations, with private data stored remotely in the hands of third parties.”).

⁵⁸ See generally Matthew C. Kelly, *Promoting the Useful Arts: Past, Current, and Future Legal Ramifications of Digital Music Piracy* (2002) (unpublished term paper, Santa Clara University) (on file with Professor David D. Friedman) *available at* http://www.daviddfriedman.com/Academic/Course_Pages/21st_century_issues/legal_issues_21_2000_pprs_web/21st_c_papers_2002/Kelly.htm (discussing infringement issues caused by “file sharing” function on OSP’s sites).

to say, the prospect of being held liable under vicarious liability constantly threatens the very existence of these online businesses.

B. Knowledge Theory under the Common Law Secondary Liability

If secondary liability jurisprudence is one of the most dynamic aspects of copyright law, the knowledge standard under contributory liability has much to be responsible for. Since its first formulation, the theory of culpable knowledge for contributory infringement has been subject to revisions in order to deal with newly arising technologies. The original nexus required holding a defendant secondarily liable gradually gave way to more liberal assertions of knowledge based on a wide variety of external circumstances.

1. The Traditional Application and Recent Changes

Early formulation of modern contributory infringement doctrine in copyright law may be attributed to two important cases, *Screen Gems-Columbia Music, Inc. v. Mark-Fi Records, Inc.*⁵⁹ and *Gershwin Publishing Corp. v. Columbia Artists Management, Inc.*⁶⁰ The shared factual pattern in both cases is that the defendants were aware of the identities of direct infringers, or had some palpable relationship with them.

In *Screen Gems*, Mark-Fi, the direct infringer of the suit, was a “fly-by-night” (i.e. shady and opportunistic) company who manufactured and sold bootleg recordings that violated plaintiffs’ copyrighted music. However, the plaintiffs also targeted numerous other defendants who had done business with Mark-Fi and were related to the broadcast of the advertisement for the infringing album.⁶¹ The plaintiffs’ central argument for pursuing secondary liability was that nocturnal companies such as Mark-Fi exist only long enough to reap “ill-gotten gains” from their infringement operation and then disappear.⁶² The District Court, however, rejected the plaintiffs’ contention that one may be liable as a contributory infringer if he “contributed to or participated or was concerned in the sale’ of the infringing records, whether with

⁵⁹ 256 F. Supp. 399 (S.D.N.Y. 1966).

⁶⁰ 443 F.2d 1159 (2d Cir. 1971).

⁶¹ *Screen Gems*, 256 F. Supp. at 401–02.

⁶² *Id.* at 404.

or without knowledge.”⁶³ The court opined that such contention would turn contributory infringement into absolute liability and turned instead to common law tort doctrine, which stipulates that only those who “knowingly participate[] in or further[] a tortious act [can be held] jointly and severally liable with the prime tort-feasor.”⁶⁴

In *Gershwin*, the defendant Columbia Artists’ Management Inc. was sued for facilitating the organization of concerts for its managed artists. The contracts between Columbia and its managed artists allowed Columbia to get a share of artists’ performance fees in compensation for its promotional efforts; however, it also turned out that some copyrighted music was performed without authorization in these concerts.⁶⁵ The Second Circuit, finding for the plaintiff, delivered a classic formulation of contributory liability: “[O]ne who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be liable as a ‘contributory infringer.’”⁶⁶

It is clear from the decisions of *Screen Gems* and *Gershwin* that providing assistance to infringing conduct will subject a facilitator to copyright liability if he does so with knowledge that his assistance materially contributes toward infringement. But, in these early cases, it was apparent that the relationship between the supplier and the user of the means was close enough to support the finding of knowledge or nexus between the contribution and infringement.⁶⁷ It is quite another matter, however, to impose the same liability when a defendant is not aware of the identity of an infringer or the nature of the

⁶³ *Id.* at 403.

⁶⁴ *Id.*; see also Jane C. Ginsburg, *Separating the Sony Sheep From the Grokster Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs*, 50 ARIZ. L. REV. 577, 580 (2008) (“Copyright infringement is a tort. So is intentionally enabling or inciting another to infringe.”).

⁶⁵ *Gershwin*, 443 F.2d at 1160–63.

⁶⁶ *Id.* at 1162.

⁶⁷ See *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 437 (1984), *superseded by statute*, Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended at 17 U.S.C.A. § 1201) (acknowledging that “‘contributory infringement’ has been applied in a number of lower court copyright cases involving an ongoing relationship between the direct infringer and the contributory infringer at the time the infringing conduct occurred”).

infringement.⁶⁸

Over time, the epistemological nexus between the nature of infringement and the identity of direct infringer started to blur. Technology enabled services and products to be widely distributed to the public where no lasting or meaningful communication between providers of technology and consumers existed beyond the point of sale. Indeed, courts seemed to have adapted to the changes. The more recent applications of contributory infringement doctrine appeared to do away with the traditional nexus pertaining to the relationship between a facilitator and the infringer.⁶⁹

However, as infringement becomes more decentralized, it becomes increasingly uncertain as to what extent a technological or service provider should be aware of infringing conducts it is alleged to have contributed. The determination of whether a given use of copyrighted work is permissible under copyright law is a very difficult endeavor from the perspective of a non-copyright holder.⁷⁰ It is simply too costly to require a provider of articles or services to distinguish between legal and illegal uses his trade may facilitate.⁷¹ Moreover, courts have interpreted the knowledge requirement for contributory copyright infringement to include both those with *actual knowledge* and those who have *constructive knowledge*—that is, having reason to know of direct infringement.⁷²

⁶⁸ Alfred C. Yen, *Sony, Tort Doctrines, and the Puzzle of Peer-to-Peer*, 55 CASE W. RES. L. REV. 815, 827 (2005).

⁶⁹ See, e.g., *Napster II*, 239 F.3d 1004, 1020 n.5 (9th Cir. 2001) (holding that Napster had actual knowledge because its co-founder admitted that Napster users are exchanging pirated music even though Napster did not have records of their real names and IP addresses).

⁷⁰ Indeed, experts' opinions regarding this question are still divided. See PAUL GOLDSTEIN, GOLDSTEIN ON COPYRIGHT, Vol. 2, § 8.1, at 8:9 n.1 (3d ed. 2008 & Supp. 2012) (suggesting that "to be liable for copyright infringement, the [alleged contributory] defendant need only have known of direct infringer's activities, and need not have reached the legal conclusion that these activities infringed a copyrighted work"); see also NIMMER & NIMMER, supra note 46, at § 12.04[A][3][b] (stating another form of contributory infringement on a party, when that party provides copyrighted work to another party despite knowing the other party's illegal intentions).

⁷¹ Judge Richard A. Posner made a useful analogy that a seller of slinky dresses whose customers include prostitutes probably should not be held liable for aiding and abetting prostitution, given the high cost of distinguishing legal and illegal uses, the high spillover costs of preventing perfectly legitimate dress sales, and his limited impact on the overall costs of prostitution. *In re Aimster*, 334 F.3d 643, 651 (7th Cir. 2003).

⁷² See *Napster II*, 239 F.3d at 1020 (discussing the necessity of having actual

As it turned out, the types of knowledge required under the contributory infringement doctrine have generated far more questions rather than answers.⁷³ They transform a determination of third-party liability into an open-ended question—especially when a challenged service or product is capable of performing or being used for more than one intended purpose.⁷⁴ The “constructive knowledge,” in particular, suggests that a service provider may be held liable if it had “general awareness” of the ongoing infringement.⁷⁵ Nonetheless, some courts have stressed that “general awareness” is not enough to establish contributory infringement, and that a more reasonably identifiable instance of infringement is required.⁷⁶ In any case, it is apparent that there should be some well-tailored exception to the application of contributory copyright liability.

2. Sony Doctrine and the Limit on Imputing Requisite Knowledge

In *Sony Corporation of America v. Universal City Studios*,⁷⁷ a case widely regarded as one of the wisest Supreme Court opinion ever rendered,⁷⁸ the Supreme Court found itself in a completely

and constructive notice to satisfy a claim).

⁷³ See JOHN W. HAZARD JR., COPYRIGHT LAW IN BUSINESS AND PRACTICE § 9:15 (2012) (demonstrating an example of how the court failed to identify the actual knowledge in case).

⁷⁴ For example, one District Court held that the sale of custom length blank tape timed to correspond to particular sound recording demonstrates that the store owner had actual knowledge of his customer’s counterfeiting activities. *A&M Records, Inc. v. Abdallah*, 948 F. Supp. 1449, 1456 (C.D. Cal. 1996).

⁷⁵ See *id.* at 1455–56 (“Under *Gershwin*, a plaintiff must prove two elements in order to establish a case of contributory liability: 1) the underlying copyright violation; and 2) the defendant knowingly induced, caused or materially contributed to that violation.”).

⁷⁶ See, e.g., *Napster II*, 239 F.3d at 1020 (holding that, in an online context, evidence of actual knowledge of specific acts of infringement is required to hold a computer system operator liable for contributory copyright infringement (citing *Religious Tech Ctr. v. Netcom On-Line Comm’n. Servs.*, 907 F. Supp. 1361, 1373 (N.D. Cal. 1995))).

⁷⁷ *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984), *superseded by statute*, Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended at 17 U.S.C.A. § 1201).

⁷⁸ See Debra A. Sitzberger, *Copyright Law—Who Gets the Picture?—Universal City Studios, Inc. v. Sony Corp. of America*, 57 WASH. L. REV. 599, 599 (1982) (“In *Universal City Studios, Inc. v. Sony Corp. of America*, the United States Court of Appeals for the Ninth Circuit defined the scope of copyright protection afforded audiovisual material broadcast on public airways.”).

different technological era.⁷⁹ In lower proceedings, it was undisputed that Sony, the distributor of the Betamax video cassette recorder (VCR), materially contributed to the purchasers' infringement because Sony's customers would not have been able to duplicate the aired programs without the VCRs.⁸⁰ The remaining problem, therefore, was whether Sony could reasonably anticipate that its product's recording function would be used to reproduce copyright protected TV programs.⁸¹

The Court, however, declined to focus on whether Sony should be held liable because it knew or should have known what its customers were up to.⁸² Instead, the Court focused some of its attention on the non-infringing uses of the VCRs.⁸³ The Court was apparently concerned that imputing a culpable knowledge on a device manufacturer might produce undesirable consequences on innovation—for it would be an equivalent of holding that the disputed article is within the exclusive domain of copyright holders.⁸⁴ In this regard, the Supreme Court looked to patent law for a more scrupulous standard in determining when a device manufacturer could be held liable for infringement committed by users of its products.⁸⁵ The outcome is the adoption of the “staple article of commerce” doctrine into copyright law to the effect that: “[T]he sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes.”⁸⁶ Pursuant to this doctrine, a device manufacturer shall not be held secondarily liable—provided that his products are “capable of substantial noninfringing [sic] uses.”⁸⁷

⁷⁹ See *id.* at 600 (describing the complicated technical surroundings of the case).

⁸⁰ *Universal City Studios v. Sony Corp. of Am.*, 659 F.2d 963, 975–76 (9th Cir. 1981).

⁸¹ See *id.* at 964–65 (stating issue I as whether “off-the-air copying of copyrighted audiovisual materials by owners of a videotape recorder in their homes for private noncommercial use constitute[s] an infringement”).

⁸² See *id.* at 975 (discussing the defendant's knowledge of Betamax's use of the product only).

⁸³ *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 421, 423–25 (1984), *superseded by statute*, Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended at 17 U.S.C.A. § 1201).

⁸⁴ *Id.* at 439, 441.

⁸⁵ See *id.* at 439 (recognizing that there is no precedent in copyright law for vicarious liability, and that patent law must be used instead).

⁸⁶ *Id.* at 442.

⁸⁷ *Id.*

The immediate effect of *Sony's* “dual use” doctrine is that constructive knowledge of infringement may not be imputed to a device manufacturer solely on the basis of its design or capability.⁸⁸ However, it should be noted that the lesson of *Sony* is not merely a matter of public policy—though many competing public interests seem to have profound effects on the *Sony* opinion.⁸⁹ Nor did the *Sony* decision only reflect the Court’s reservation to depart from contributory infringement precedent—that there be some continuing relationship beyond the point of sale before courts can impose such liability.⁹⁰ The true lesson of *Sony* is probably that courts should not allow copyright owners to establish indirect copyright liability on the basis of general awareness.⁹¹

According to the *Sony* Court the only theory to support Sony’s vicarious or contributory liability in this case “must rest on the fact that [Sony has] sold equipment with constructive knowledge of the fact that [its] customers may use that equipment to make unauthorized copies of copyrighted material.”⁹² The Court, however, went on to hold that there is no precedent in copyright law to support such theory.⁹³ In this regard, the Court implicitly suggested that the “general awareness” of infringement could not

⁸⁸ Compare *id.* at 436–38, with Brad Polizzano, Note, *Grokster Not the “Spirit in the Sky” Innovators Long for: Uncertain Protection “Forever Young” Since the Birth of Peer-to-Peer*, 83 ST. JOHN’S L. REV. 635, 637 (2009) (indicating that constructive knowledge is not sufficient to find a manufacturer vicariously liable according to the *Sony* case).

⁸⁹ See *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 430–31 (1984), *superseded by statute*, Digital Millennium Copyright Act, Pub. L. No. 105–304, 112 Stat. 2860 (1998) (codified as amended at 17 U.S.C.A. § 1201) (noting that it is the responsibility of Congress, and not the courts, to expand the scope of copyright protection); see Daryl J. Levinson, *Aimster and Optimal Targeting*, 120 HARV. L. REV. 1148, 1150 (2007) (“For indirect liability to be efficient . . . the target of indirect liability must be capable of controlling wrongdoing in some cost-effective way.”).

⁹⁰ See *Sony*, 464 U.S. at 437–39 (noting that a contract was formed between Sony and its customers when they purchased the Betamax which condemned using the machine to copy copyrighted materials, and also pointing out that copyright law did not apply to the case).

⁹¹ See *id.* at 439–40 (“The prohibition against contributory infringement is confined to the knowing sale of a component especially made for use in connection with a particular patent. There is no suggestion in the statute that one patentee may object to the sale of a product that might be used in connection with other patents.”); see also Polizzano *supra* note 88, at 637 (indicating that constructive knowledge is not sufficient to find a manufacturer vicariously liable according to the *Sony* case).

⁹² *Sony*, 464 U.S. at 439.

⁹³ *Id.*

bring about secondary liability under copyright law.⁹⁴ It follows, therefore, that both contributory infringement and vicarious liability must be based on some readily identifiable instances of infringement rather than general knowledge.⁹⁵ Unfortunately, this aspect of *Sony* is neither sufficiently understood nor well received among commentators and courts.⁹⁶ The *Sony* Court's suggestion did not seem to have demonstrable effects on subsequent interpretation of requisite knowledge standard in contributory infringement jurisprudence.⁹⁷

Nonetheless, the safe-harbor aspect of the *Sony* decision provides many puzzles for future application.⁹⁸ On close examination, *Sony's* rule turns out to be less clear and straightforward than its underlying staple article of commerce doctrine might suggest.⁹⁹ In the first place, the *Sony* Court's choice in borrowing a concept from patent law, instead of going back to tort law of enterprise liability, is doubtful.¹⁰⁰ It is rather difficult to see how "commodities of commerce" such as VCRs or

⁹⁴ *Id.* at 438; see also Polizzano, *supra* note 88, at 637 (indicating that constructive knowledge is not sufficient to find a manufacturer vicariously liable according to the *Sony* case).

⁹⁵ *Sony*, 464 U.S. at 439.

⁹⁶ See, e.g., *Artista Records LLC v. Lime Grp. LLC*, 784 F. Supp. 2d 398, 434 (S.D.N.Y. 2011) (subjecting Limewire to the "*Sony-Betamax*" standard only if Limewire fails to demonstrate that their software platform is used overwhelmingly for non-infringing uses, such as sharing of personal or non-proprietary documents or files (citing *Sony*, 464 U.S. at 442)).

⁹⁷ See, e.g., *A&M Records, Inc. v. Napster, Inc. (Napster I)*, 114 F. Supp. 2d 896, 918 (N.D. Cal. 2000) (holding that copyright law does not require actual knowledge of a specific infringing act for contributory infringement to exist). This decision was subsequently overruled by the Ninth Circuit in *Napster II*. However, the Ninth Circuit derived a conclusion that specific knowledge of infringement is required from *Religious Technology Center* and not *Sony*. See *Napster II*, 239 F.3d 1004, 1021 (9th Cir. 2001) (agreeing with *Netcom* court that "in an online context, evidence of actual knowledge of specific acts of infringement is required to hold a computer system operator liable for contributory copyright infringement" (citing *Religious Tech. Ctr. v. Netcom Online Commc'n Servs., Inc.*, 907 F. Supp. 1361, 1373 (N. D. Cal. 1995))).

⁹⁸ See Peter S. Menell & David Nimmer, *Unwinding Sony*, 95 CALIF. L. REV. 941, 944–45, 1022, 1024 (2007) (explaining how the creation of the safe-harbor out of patent law instead of using tort law had far-reaching effects on future copyright policy and law).

⁹⁹ See *id.* at 977–79 (giving an example of how the use and construction of the safe-harbor provision as part of the staple article of commerce doctrine by the Court was unclear and "vague").

¹⁰⁰ See Peter S. Menell & David Nimmer, *Legal Realism in Action: Indirect Copyright Liability's Continuing Tort Framework and Sony's De Facto Demise*, 5 UCLA L. REV. 143, 156 (2007) (arguing that the *Sony* Court's turn to patent law, rather than tort law, is a major cause of confusion).

copying machines—products whose main functionality is to empower users to override a copyright holder’s exclusive authority to make copies—could be deemed capable of “substantial’ non-infringing use.”¹⁰¹ Indeed, since its inception, the *Sony* doctrine has not been able to immunize any company from indirect liability.¹⁰² Furthermore, when it devised the *Sony* safe harbor, the *Sony* Court seemed to conflate the staple article of commerce and the inducement liability together under patent law.¹⁰³ This makes it difficult to separate an analysis of defendant’s knowledge from that of intent. From this perspective, therefore, the *Sony* decision—as generally interpreted—provides far less clarification with regard to the application of contributory infringement than its supporters had hoped.¹⁰⁴

In addition, subsequent courts have held that the *Sony* doctrine applies only to the product distribution model—where a defendant was unaware of specific infringement and had no continuing relationship with the users.¹⁰⁵ This interpretation of *Sony*’s rule significantly reduces the value of the dual-use defense for modern cloud-based service providers.¹⁰⁶

¹⁰¹ *See id.* at 176 (quoting *A&M Records, Inc. v. Abdullah*, 948 F. Supp. 1449, 1456 (C.D. Cal. 1996)).

¹⁰² *Id.* at 145 (“[N]o reported decision has found the *Sony* safe harbor to immunize a technology company accused of indirect liability.”).

¹⁰³ *See Grokster I*, 545 U.S. 913, 936–37 (2005) (indicating the relationship between the staple article of commerce within the *Sony* case safe harbor and inducement liability). The inducement liability and contributory liability (staple article of commerce doctrine) under patent law are coded separately as 35 U.S.C. §§ 271(b) and 271(c), respectively. 35 U.S.C.A. § 271(b), (c) (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/07/12). However, “induced infringement was not considered a separate theory of indirect liability in the pre-1952 case law . . . it was treated as evidence of ‘contributory infringement.’” *Global-Tech Appliances, Inc. v. SEB S.A.*, 131 S. Ct. 2060, 2067 (2011). It was the Congress which separated the contributory infringement concept into two categories, i.e. induced infringement under § 271(b), and sale of a component of a patented invention under § 271(c). *Id.*

¹⁰⁴ *See Menell & Nimmer, supra* note 100, at 187 (stating that the *Sony* decision “has proven to be shaky and vague Supreme Court precedent”).

¹⁰⁵ *Arista Records LLC v. Usenet.com, Inc.*, 633 F. Supp. 2d 124, 156 (S.D.N.Y. 2009); *Capitol Records*, 821 F. Supp. 2d 627, 649 (2011) (S.D.N.Y. 2011).

¹⁰⁶ *See Arista Records LLC*, 633 F. Supp. 2d at 155, 156 (noting that defendants “maintain an ongoing relationship with their users” and holding them liable for contributory infringement); *Capitol Records*, 821 F. Supp. 2d at 646, 648 (discussing the method by which the court determines whether a defendant should be held contributorily liable for copyright infringement).

3. The Ninth Circuit's Interpretation of *Sony* Doctrine in *Napster*

The substantial non-infringing use doctrine under *Sony* met its limitation for the first time in *A&M Records, Inc. v. Napster, Inc.*¹⁰⁷ In *Napster*, the Ninth Circuit held that *Sony*'s dual-use defense does not apply if an alleged contributory infringing defendant had actual and constructive knowledge of direct infringement proven through means other than the design of disputed products.¹⁰⁸ Moreover, the *Napster* court separately considered Napster's material contribution to the infringement, finding that "Napster provides the 'site and facilities' for direct infringement."¹⁰⁹ Thus, while the court deemed Napster's architecture to be within the ambit of *Sony*'s safe harbor, it held that Napster's *participation* in the infringement by actually operating the file-sharing system lay outside the staple article of commerce doctrine.¹¹⁰

One can notice without much difficulty that the *Napster* court's reading of *Sony* has turned the dual-use doctrine into a technology-specific defense—it determined that the *Sony* defense applies only when a defendant is an operator of a service and not a distributor at the same time.¹¹¹ The *Napster* court once again liberated the scope of contributory liability by allowing a wide possibility of imputing culpable knowledge against technological providers.¹¹² In this regard, the Ninth Circuit's holding in *Napster* put in place an *ex-ante* incentive for the next generation of providers of file-sharing technology to implement a hands-off approach that would leave the Internet a fertile place for piracy.¹¹³

4. *In re Aimster* and Doctrine of Willful Blindness

Sony's defense was further curtailed in another file-sharing dispute—*In re Aimster Copyright Litigation*.¹¹⁴ *Aimster* put the contributory infringement doctrine to a difficult test by asking

¹⁰⁷ *Napster II*, 239 F.3d 1004, 1020–22 (9th Cir. 2001).

¹⁰⁸ *Id.* at 1021–22 (holding that Napster's actual, specific knowledge of direct infringement necessarily precludes Napster from relying on *Sony*'s defense).

¹⁰⁹ *Id.* at 1022.

¹¹⁰ *Id.* at 1021–22.

¹¹¹ *Id.* at 1019.

¹¹² *Id.* at 1021–22.

¹¹³ Ginsburg, *supra* note 64, at 582–83.

¹¹⁴ *In re Aimster*, 334 F.3d 643, 647, 649 (7th Cir. 2003).

whether *Sony's* dual-use defense could apply if a provider chooses to evade the knowledge of infringement by choice rather than by architectural necessity.¹¹⁵ Design-wise, *Aimster's* file-sharing service differed from previous predecessors in that it included an encryption feature into its freely downloadable software which rendered all communication between users encrypted.¹¹⁶

Judge Richard Posner of the Seventh Circuit chipped away the weight of *Sony* defense in two significant ways.¹¹⁷ First, the *Aimster* court—confident that *Sony's* standard calls for a strict cost-benefit analysis—declared that mere evidence that a product or service is physically *capable* of non-infringing use is not enough to invoke the *Sony* defense.¹¹⁸ In this regard, the court rejected *Aimster's* over-reaching argument that it should be eligible for the *Sony* defense upon mere showing that “its file-sharing system *could* be used in noninfringing ways.”¹¹⁹ The court then reached its decision at the other extreme and held that *Aimster* was secondarily liable due to its failure in showing that its service was *actually* used for any claimed non-infringing purpose.¹²⁰ Judge Posner, in addition, went on to assert that even if *Aimster* could make such a showing, it would still not be unhinged from contributory infringement unless it was able to demonstrate that “it would have been disproportionately costly . . . to eliminate or at least reduce substantially the infringing uses.”¹²¹

In this respect, Judge Posner's analysis appeared to be primarily out of a policy concern based on an economic theory which renders the court's application of contributory liability highly contextualized rather than generalized.¹²² According to the Circuit Judge, an ISP should not be allowed to easily push aside its responsibility to prevent further wrongful conduct and eschew

¹¹⁵ *Id.* at 650.

¹¹⁶ *Id.* at 646.

¹¹⁷ *Id.* at 651, 653.

¹¹⁸ *Id.* at 653.

¹¹⁹ *In re Aimster*, 334 F.3d 643, 651 (7th Cir. 2003) (“Were that the law, the seller of a product or service used *solely* to facilitate copyright infringement, though it was capable in principle of noninfringing uses, would be immune from liability for contributory infringement.”).

¹²⁰ *Id.* at 653.

¹²¹ *Id.*

¹²² *See id.* (“Even when there are noninfringing uses . . . if the infringing uses are substantial then to avoid liability as a contributory infringer the provider of the service must show that it would have been disproportionately costly for him to eliminate or at least reduce substantially the infringing uses.”).

its unique position as the “least cost avoider.”¹²³ This reasoning thus somehow expands contributory liability in the context of online infringement and, in effect, puts a stop to any reasonable application of *Sony’s* doctrine.¹²⁴

The real trouble, however, is the court’s response to John Deep’s argument that Aimster could not have actual knowledge of the infringement because the software’s encryption feature rendered it impossible for Deep to know what works were being infringed by the users.¹²⁵ Judge Posner rejected Deep’s argument as a transparent, head-in-the-sand, tactic to ditch one’s responsibilities and concluded that Aimster could not avail itself of the benefit of *Sony’s* defense by purposefully avoiding acquiring the actual knowledge of infringing activities.¹²⁶

The principle that “willful blindness” equates to actual knowledge may sound rather counter-intuitive.¹²⁷ However, “willful blindness” or “deliberate ignorance” has been a well-established doctrine in “both British and American criminal jurisprudence for over a century.”¹²⁸ This concept has been referred to in criminal cases under various nomenclatures, such “as connivance, conscious avoidance, constructive knowledge, deliberate ignorance, deliberate or willful shutting of the eyes, knowledge of the second degree, purposely abstaining from ascertaining and studied ignorance.”¹²⁹ In *Aimster*, Judge Posner affirmatively held that “[w]illful blindness is knowledge, in copyright law [where indeed it may be enough that the defendant *should* have known of the direct infringement.”¹³⁰

Nonetheless, the *Aimster* court did not declare that the blind eye theory alone would suffice to establish contributory liability against a service provider.¹³¹ Rather, the court seemed to suggest

¹²³ *Id.* at 655; Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 390–91 (2005).

¹²⁴ *See In re Aimster*, 334 F.3d at 648, 655 (explaining that “the service provider must do what it can reasonably be asked to do to prevent the use of its service by ‘repeat infringers’”).

¹²⁵ *Id.* at 650.

¹²⁶ *Id.*

¹²⁷ *See id.*

¹²⁸ Tal S. Benschar et al., *Proving Willfulness in Trademark Counterfeiting Cases*, 27 Colum. J.L. & Arts 121, 123 (2003).

¹²⁹ *Id.* at 124.

¹³⁰ *In re Aimster*, 334 F.3d at 650 (citing *Casella v. Morris*, 820 F.2d 362, 365 (11th Cir. 1987)).

¹³¹ *See id.* at 645–56 (failing to state that willful blindness alone would constitute contributory liability).

that some scienter is required to hold an alleged contributory defendant liable—and willful blindness serves as an invitation for courts to discern such provider’s ill intent—in the face of obvious and abundant information regarding direct infringement.¹³²

Many trademark decisions have dealt with the concept of willful blindness and have suggested that the doctrine has something to do with a failure to investigate the infringement.¹³³ In *Louis Vuitton S.A. v. Lee*, the Seventh Circuit held that willful blindness results from the defendant’s failure to “inquire further because he was afraid of what the inquiry would yield.”¹³⁴ In another Seventh Circuit decision, *Hard Rock Cafe Licensing Corp. v. Concession Services, Inc.*, the court likewise confirmed that “[t]o be willfully blind, a person must suspect wrongdoing and deliberately fail to investigate.”¹³⁵ It is, however, unclear as to what extent these decisions could lend their interpretations of the willful blindness doctrine to the context of indirect copyright infringement.¹³⁶ But a suggestion that online service providers may have an intrinsic and general duty to investigate infringement is a bad policy for online innovation.¹³⁷ It goes against the grain for online communication, in general, to imply that content of electronic communication may be subjected to routine monitoring for the purpose of copyright enforcement.¹³⁸

¹³² See *id.* at 650 (The defendant could not escape liability “by using encryption software to prevent himself from learning what surely he strongly suspects to be the case: that the users of his service—maybe *all* the users of his service—are copyright infringers.”).

¹³³ *E.g.*, *Hard Rock Cafe Licensing Corp. v. Concession Serv., Inc.*, 955 F.2d 1143, 1149 (7th Cir. 1992); *Louis Vuitton S.A. v. Lee*, 875 F.2d 584, 590 (7th Cir. 1989).

¹³⁴ *Louis Vuitton S.A.*, 875 F.2d at 590.

¹³⁵ *Hard Rock Cafe Licensing Corp.*, 955 F.2d at 1149 (citing *Louis Vuitton S.A.*, 875 F.2d at 590).

¹³⁶ The Supreme Court has warned that there are fundamental differences between copyright and trademark law; thus the Court would not look to standards for contributory infringement in trademark authorities for the purpose of adoption in copyright disputes. *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 439 & n.19 (1984), *superseded by statute*, Digital Millennium Copyright Act, Pub. L. No. 105–304, 112 Stat. 2860 (1998) (codified as amended at 17 U.S.C.A. § 1201).

¹³⁷ See *Grokster I*, 545 U.S. 913, 957 (2005) (Breyer, J., concurring) (“*Sony’s rule is strongly technology protecting.*”).

¹³⁸ Article 15(1) of the European E-Commerce Directive imposes neither a general duty to monitor the information which ISPs transmit or store, “nor a general obligation actively to seek facts or circumstances indicating illegal activity.” Council Directive 2000/31, art. 15, 2000 O.J. (L 178) 13 (EC).

The Supreme Court rarely has had an opportunity to consider the issue of willful blindness in the context of indirect infringement liability.¹³⁹ However, in *Global-Tech Appliances, Inc. v. SEB S.A.*¹⁴⁰—a recent Supreme Court’s deliberation on a patent dispute involving the issue of inducement liability in a cool frying-pan patent—the Supreme Court held that the knowledge element for a claim of willful induced patent infringement can be fulfilled by a showing of willful blindness.¹⁴¹

The *Global-Tech* Court confirmed that the willful blindness doctrine could be used to support a finding of knowledge in patent contributory liability, as well as inducement liability.¹⁴² According to the Court, “defendants who behave in this manner are just as culpable as those who have actual knowledge.”¹⁴³ After a lengthy discussion of circumstances under which the doctrine of willful blindness may be invoked,¹⁴⁴ the Court concluded by providing a definitive formulation of the doctrine: “[A] willfully blind defendant is one who takes deliberate actions to *avoid confirming* a high probability of wrongdoing and who can almost be said to have actually known the critical facts.”¹⁴⁵

The Court also supported previous Circuits’ articulations of the doctrine that a “defendant must subjectively believe that there is a high probability that a fact [pertaining to direct infringement] exists.”¹⁴⁶ As explained by the Court, the subjective nature of the awareness is required to ensure that willful blindness will not be imposed upon mere recklessness or negligence.¹⁴⁷ At first glance, the precise threshold of the subjective awareness element appears to be rather uncertain.¹⁴⁸ Among the Circuits’ decisions cited by the Court, it is sometimes said that “strong suspicion of wrongdoing” may trigger the willful blindness doctrine.¹⁴⁹ In order to dispel confusion, the *Global-Tech* Court remarked that

¹³⁹ See *Global-Tech Appliances*, 131 S. Ct. 2060, 2069 (2011) (adopting the willful blindness doctrine in the context of induced patent infringement).

¹⁴⁰ 131 S. Ct. 2060 (2011).

¹⁴¹ *Id.* at 2069, 2072.

¹⁴² *Id.* at 2068.

¹⁴³ *Id.* at 2069.

¹⁴⁴ *Id.* at 2069–70.

¹⁴⁵ *Id.* at 2070–71 (emphasis added).

¹⁴⁶ *Global-Tech Appliances*, 131 S. Ct. 2060, 2070 (2011).

¹⁴⁷ *Id.* at 2070–71.

¹⁴⁸ See *id.* (explaining the subtle differences between willful blindness, recklessness, and negligence).

¹⁴⁹ *Id.* at 2070 n.9 (quoting *United States v. Draves*, 103 F.3d 1328, 1333 (7th Cir. 1997)).

merely being aware of a substantial, albeit unjustified, risk of wrongdoing, or that a defendant “should have known of a similar risk,” would not satisfy the willful blindness standard for the requisite state of mind.¹⁵⁰ The Court then settled the rule that willful blindness can be found only where “it can almost be said that the defendant *actually knew*.”¹⁵¹

Pursuant to the articulation of the willful blindness doctrine by the Supreme Court in *Global-Tech*, some inferences in relation to the knowledge element under contributory infringement may reasonably be drawn.¹⁵² First, congruent with the Seventh Circuit’s rendition of the doctrine in trademark context, the *Global-Tech* Court suggests that an alleged indirect infringement defendant may find herself with a duty to investigate or confirm the facts of direct infringement, whenever existing information is enough to signal a high probability of wrong doing.¹⁵³ Secondly, while willful blindness appears to require a high standard of personal knowledge, the most important element is that defendants take “deliberate action to avoid learning of that fact.”¹⁵⁴ Thus, mere “deliberate indifference” would not lead to a finding of willful blindness.¹⁵⁵ Thirdly, and perhaps most important, the doctrine’s focus on deliberate action to avoid the confirmation of critical fact renders willful blindness a seemingly separate inquiry into the intent of a non-direct infringer, rather than a means to establish requisite knowledge.¹⁵⁶

Returning to the copyright context, it is still not clear how the

¹⁵⁰ *Id.* at 2071.

¹⁵¹ *Id.* (emphasis added) (quoting GLANVILLE WILLIAMS, CRIMINAL LAW § 57 (2d ed. 1961)).

¹⁵² *Global-Tech Appliances*, 131 S. Ct. 2060, 2070–71 (2011).

¹⁵³ *Id.* at 2070–71, 2070 n.9. The notion that willful blindness requires a “failure to investigate” also appears in criminal cases. *See* United States v. Florez, 368 F.3d 1042, 1044 (8th Cir. 2004) (“Ignorance is deliberate if the defendant was presented with facts that put her on notice that criminal activity was particularly likely and yet she intentionally failed to investigate those facts.”). However, it is not clear whether such a concept could be transposed to the context of contributory infringement involving intellectual property rights.

¹⁵⁴ *Global-Tech Appliances*, 131 S. Ct. at 2070–71.

¹⁵⁵ *Id.* at 2068.

¹⁵⁶ *See id.* at 2068–69 (“[C]ourts applying the doctrine of willful blindness hold that defendants cannot escape [liability] . . . by deliberately shielding themselves from clear evidence of critical facts that are strongly suggested by the circumstances. . . . It is also said that persons who know enough to blind themselves to direct proof of critical facts in effect have actual knowledge of those facts.”).

willfully blind stand in relation to the *Sony* doctrine.¹⁵⁷ In *Aimster*, John Deep's decision to implement an encryption feature into Aimster's software package was determined to be a deliberate action to blind himself from the illicit file-sharing in which Aimster's users had been engaged.¹⁵⁸ However, any design feature with the purpose of limiting a developer's responsibility could similarly be held to be such a probative step.¹⁵⁹ Unfortunately, the Supreme Court in *MGM v. Grokster* refused to provide a useful clue to this puzzle.¹⁶⁰ Indeed, as the *Global-Tech* Court explained, the Supreme Court had no need to discuss the willful blindness doctrine in *Grokster*, since the Court in that case "found ample evidence that Grokster and StreamCast were fully aware—in the ordinary sense of the term—that their file-sharing software was routinely used in carrying out the acts that constituted infringement . . . and that these acts violated the rights of copyright holders."¹⁶¹

The corollaries set forth above also connote difficulty in the application of the *Global-Tech* Court's willful blindness doctrine in the copyright infringement context. In formulating the doctrine of willful blindness, the *Global-Tech* Court did not discuss potential impacts of this concept on the staple article of commerce doctrine.¹⁶² It is therefore highly questionable as to how the willful blindness doctrine would stand in light of *Sony's* defense.¹⁶³ On one hand, the implied duty to investigate upon a

¹⁵⁷ See, e.g., *In re Aimster*, 334 F.3d 643, 653 (7th Cir. 2003) ("Aimster blinded itself in the hope that by doing so it might come within the rule of the *Sony* decision.").

¹⁵⁸ *Id.* at 650.

¹⁵⁹ See *Grokster I*, 545 U.S. 913, 933 (2005) ("*Sony* barred secondary liability based on presuming or imputing intent to cause infringement solely from the design or distribution of a product capable of substantial lawful use, which the distributor knows is in fact used for infringement.>").

¹⁶⁰ See generally *id.* at 913–66 (failing to address design features as limiting a developer's responsibility).

¹⁶¹ *Global-Tech Appliances*, 131 S. Ct. at 2070.

¹⁶² This is because Pentalpha, the defendant in *Global-Tech Appliances*, did not raise any argument that the product it had been actively inducing to be imported into the U.S. was capable of substantial non-infringing use. See *id.* at 2064, 2065, 2070 (stating Pentalpha's arguments, which related only to induced infringement). In any case, the staple article of commerce doctrine in patent law only applies to a sale or importation of a key "component" of a patented product or process, and not to an infringing device itself. 35 U.S.C.A. § 271(c) (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/07/12); *Global-Tech Appliances*, 131 S. Ct. at 2067.

¹⁶³ *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 442 (1984), *superseded by statute*, Digital Millennium Copyright Act, Pub. L. No.

“high probability of wrongdoing” is simply an outright contradiction to the philosophy of the *Sony* doctrine, which provides a safe harbor for technological providers, by foreclosing the imputation of requisite knowledge—where the product or service is capable of substantial non-infringing uses.¹⁶⁴ On the other hand, the true nature of the willful blindness doctrine is not a separate theory of knowledge for indirect infringement analysis, but rather a tool for determining the culpable intent of a defendant.¹⁶⁵ Indeed, as was made clear by the Supreme Court in *Global-Tech Appliances*, the determination of willful blindness always requires further affirmative steps or deliberate actions on the part of a defendant so as to avoid confirming the knowledge she subjectively entertains.¹⁶⁶ The willful blindness doctrine thus undermines the importance of the substantial non-infringing uses inquiry, by directing courts’ attention to a service provider’s indifference with regard to on-going infringement.¹⁶⁷

5. *Grokster* and Copyright Inducement Liability

The common law development of a knowledge requirement for contributory copyright liability reached its high point in the Supreme Court’s 2005 decision in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*¹⁶⁸ Defendant Grokster’s software utilized “FastTrack” networking technology, which selects user computers on the network to act as indexing servers, thereby eliminating the need for a service provider to maintain central indexing servers.¹⁶⁹ This decentralized architecture thus allowed users to store and search for file information without any aid from Grokster.¹⁷⁰ Furthermore, Grokster did not demand that

105–304, 112 Stat. 2860 (1998) (codified as amended at 17 U.S.C.A. § 1201).

¹⁶⁴ See *Global-Tech Appliances*, 131 S. Ct. at 2070 (defining a willfully blind defendant); *Sony*, 464 U.S. at 491 (“[I]f a *significant* portion of the product’s use is *noninfringing*, the manufacturers and sellers cannot be held contributorily liable for the product’s infringing uses.”).

¹⁶⁵ See *Global-Tech Appliances*, 131 S. Ct. at 2070–71 (describing the willful blindness doctrine).

¹⁶⁶ *Id.* at 2072.

¹⁶⁷ See *In re Aimster*, 334 F.3d 643, 650 (7th Cir. 2003) (stating that the service provider’s “[w]illful blindness is knowledge” within the copyright law context).

¹⁶⁸ See *Grokster I*, 545 U.S. 913, 941 (2005) (discussing the holding in *Sony*, which included a knowledge requirement for liability).

¹⁶⁹ *Grokster II*, 380 F.3d 1154, 1159 (9th Cir. 2004), *vacated and remanded by* 545 U.S. 913 (2005).

¹⁷⁰ *Id.* at 1159–60.

users must register or provide authenticating information before they could swap files through Grokster's software.¹⁷¹ Grokster, therefore, did not know when a particular file was copied and also lacked the ability to either block access by users or to track their behaviors on its networks.¹⁷²

These decentralized aspects of Grokster forced the Supreme Court to reconsider the tension between imposing liability on the distributors of infringement-facilitating software and the need for maintaining a clear exemption to liability that will foster technological development.¹⁷³ Indeed, in his concurring opinion, Justice Breyer viewed the real question in *Grokster* to be whether the Court should modify the *Sony* standard, pursuant to the plaintiff copyright owners' request, or interpret *Sony* more strictly, following Justice Ginsburg's approach.¹⁷⁴

The *Grokster* Court resolved the issue by asserting a re-reading of *Sony's* mandate.¹⁷⁵ According to the Court, *Sony's* staple article of commerce doctrine is a compromise that limits liability to "instances of more acute fault," as opposed to the "mere understanding that some of one's products will be" put to unlawful uses.¹⁷⁶ The Court thus rejected the Ninth Circuit's interpretation of *Sony* as a broad defense against imposition of indirect copyright liability in a case where a distributed product or service is capable of substantial non-infringing uses, unless the distributor had "specific knowledge of infringement," and "failed to act upon that information."¹⁷⁷ The Court clarified that *Sony* only inures a distributor against secondary liability by preventing the finding of presumed intent to cause infringement based solely on the "design or distribution of a product capable of substantial lawful use, which the distributor knows is in fact used for infringement."¹⁷⁸ Accordingly, when a distributor's culpable intent could be demonstrated through means other than the characteristics or uses of a distributed product, a court may

¹⁷¹ *Grokster I*, 545 U.S. at 928.

¹⁷² *See Grokster II*, 380 F.3d at 1165 (stating that the evidence, presented by the parties, showed that the defendants could neither block nor control usage of the file sharing software at issue in the case).

¹⁷³ *Grokster I*, 545 U.S. at 928–929.

¹⁷⁴ *Id.* at 956 (Breyer, J., concurring).

¹⁷⁵ *See id.* at 933–34 (describing the Court's interpretation of *Sony's* mandate).

¹⁷⁶ *Id.* at 932–33.

¹⁷⁷ *Id.* at 933–934 (quoting *Grokster II*, 380 F.3d at 1162).

¹⁷⁸ *Id.* at 933.

not ignore this evidence.¹⁷⁹

It should be noted that the *Grokster* decision did not actually object to the Ninth Circuit's reading of *Sony* that actual knowledge of specific infringement is required to hold a device distributor liable where its product falls within the ambit of the staple article of commerce doctrine.¹⁸⁰ The import of *Grokster's* rule is that it dissolved the traditional nexus between knowledge of infringement and the ability of a service provider to do something about the ongoing violation of exclusive rights—which had long been the central premise of contributory liability¹⁸¹—by introducing inducement liability into copyright law.¹⁸²

Unlike the Seventh Circuit, however, the *Grokster* Court did not employ the blind eye theory to solve the puzzle of decentralized P2P architecture.¹⁸³ In subjecting *Grokster* to secondary liability, the *Grokster* Court adopted the following rule: “one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.”¹⁸⁴ The *Grokster* Court thus replaced the Ninth Circuit's analytical approach of assessing level of knowledge with a theory that “premises liability on purposeful, culpable expression and conduct” of a third-party manufacturer.¹⁸⁵

It is worth emphasizing that, according to the *Grokster* Court's unanimous opinion, the inclusion of inducement liability into copyright law was not an aberration from the *Sony* doctrine.¹⁸⁶ On the contrary, the *Grokster* decision merely articulated what

¹⁷⁹ *Grokster I*, 545 U.S. 913, 935–36 (2005).

¹⁸⁰ *See id.* at 933–34, 937 (explaining that under *Sony*, “mere knowledge of infringing potential or of actual infringing uses would not be enough here to subject a distributor to liability”).

¹⁸¹ *See* NIMMER & NIMMER, *supra* note 46, at § 12.04[A][2], [A][4][a], [A][4][b] (describing the effects of the rule from *Grokster*).

¹⁸² *Id.* § 12.04[A][5][a].

¹⁸³ *See Global-Tech Appliances*, 131 S. Ct. 2060, 2070 (2011) (explaining that the *Grokster* Court “had no need to consider the doctrine of willful blindness” because there was “ample evidence that [the defendants] were fully aware . . . that their file-sharing software was routinely used in carrying out acts that constituted infringement”).

¹⁸⁴ *Grokster I*, 545 U.S. at 936–37.

¹⁸⁵ *Id.* at 934, 937.

¹⁸⁶ *See id.* at 936–37 (stating that “the inducement rule . . . is a sensible one for copyright”).

the Supreme Court in *Sony* had not.¹⁸⁷ This is not an altogether arbitrary reasoning. The *Sony* Court's heavy reliance on patent law for the staple article of commerce doctrine, coupled with the historical origin of contributory and inducement liability as discussed above, inevitably lends much credence to a conclusion that inducement liability is a necessary component of third-party liability analysis.¹⁸⁸

Nonetheless, it is undeniable that *Grokster's* inducement rule does turn a gatekeeper into a "wrongdoer in its own right."¹⁸⁹ Under *Grokster*, an ISP would be guilty if it induces its users to infringe copyrights by taking "active steps" to encourage direct infringement.¹⁹⁰ While recasting third-party gatekeepers as principal culprits may provide an efficient solution to the online piracy problem,¹⁹¹ this approach undoubtedly disturbs the traditional distinction between parties who actually infringe copyrights and those who merely assist.¹⁹² In this regard, it is difficult to reconcile the *Grokster* Court's clarification of *Sony* with what Justice Breyer claimed to be the tenets of *Sony's* dual-use doctrine:

Sony thereby recognizes that the copyright laws are not intended to discourage or to control the emergence of new technologies, including (perhaps especially) those that help disseminate information and ideas more broadly or more efficiently. Thus *Sony's* rule shelters VCRs, typewriters, tape recorders, photocopiers, computers, cassette players, compact disc burners, digital video recorders, MP3 players, Internet search engines, and peer-to-peer software.¹⁹³

More significantly, the *Grokster* Court's weakening of *Sony's* directive destroys the balance of common law secondary liability by expanding the scope of gatekeepers' responsibility while

¹⁸⁷ See *id.* at 934–35 (“[N]othing in *Sony* requires courts to ignore evidence of intent if there is such evidence, and the case was never meant to foreclose rules of fault-based liability derived from the common law.”).

¹⁸⁸ *Id.* at 936, 937.

¹⁸⁹ Levinson, *supra* note 89, at 1152–53.

¹⁹⁰ *Grokster I*, 545 U.S. at 936.

¹⁹¹ See Levinson, *supra* note 89, at 1152–53 (explaining that “forcing *Grokster* to redesign its software to allow it to block illegal uses or to shut itself down entirely was a more efficient way of preventing copyright violations than targeting individual infringers”).

¹⁹² See *id.* (stating that the more efficient approach of merely recasting *Grokster* as a wrongdoer “would not be a sufficient basis for imposing indirect liability”).

¹⁹³ *Grokster I*, 545 U.S. at 957 (Breyer, J., concurring).

marginalizing their central defense.¹⁹⁴ *Grokster* purports to clarify the scope of the staple article of commerce doctrine in *Sony*, but instead adopts a separate theory for imposing liability on a third party, based on that party's intent as manifested by external indicia.¹⁹⁵ Some of these indicia, however, more closely resemble an indication of willful ignorance rather than intent to induce.¹⁹⁶ *Grokster's* ambiguity also leads to an appalling conclusion that providers' failure to invigilate over the course of their operation may give rise to probative inducement claim.¹⁹⁷ In this regard, the *Grokster* Court's failure to provide a clear definition as to what constitutes "active inducement" significantly complicates the traditional determination of knowledge in indirect copyright liability jurisprudence.¹⁹⁸ It literally empowers copyright owners—by providing a hunting license to impose indirect liability in a wide variety of circumstances—with the right to "veto" new media.¹⁹⁹ As a consequence, this curious inter-play between knowledge of contributory liability and the "intent" to induce necessarily relegates *Sony's* safe harbor into oblivion and forces OSPs to look elsewhere for meaningful safe harbors.²⁰⁰

¹⁹⁴ See *id.* at 9334–35, 936–37 (finding that the *Sony* rule does not limit third-party liability when there is evidence of inducement).

¹⁹⁵ See *id.* at 936–37 (explaining that evidence of "purposeful, culpable expression and conduct" will result in third party liability).

¹⁹⁶ For example, the Court remarked that while *Grokster* and *StreamCast* may not have an independent duty to monitor their users' activities, their failure to develop filtering tools and other infringement-diminishing mechanisms "underscores [their] intentional facilitation of their users' infringement." *Id.* at 939.

¹⁹⁷ While the Court opined that "failure to take affirmative steps to prevent infringement" alone may not furnish adequate evidence of intent where the device was capable of substantial non-infringing uses, the Court did not mention whether such failure would, nonetheless, be enough to establish knowledge under the willful blindness doctrine. *Id.* at 939 n.12.

¹⁹⁸ *Id.* at 939 n.12, 942 (Ginsburg, J., concurring).

¹⁹⁹ NEIL WEINSTOCK NETANEL, COPYRIGHT'S PARADOX 79 (2008) (arguing that *Grokster's* holding enables copyright owners to block innovations that threaten to jeopardize their business model).

²⁰⁰ See *id.* at 78 (explaining how the *Grokster* decision destroyed the staple supplier safe harbor created by the *Sony* decision).

III. SAFE HARBORS UNDER THE DIGITAL MILLENNIUM COPYRIGHT ACT

A. Purpose & Background

Congress passed the Digital Millennium Copyright Act in 1998 to implement the two new landmark World Intellectual Property Organization (WIPO) treaties—the WIPO Copyright Treaty (WCT)²⁰¹ and the WIPO Performances and Phonograms Treaty (WPPT).²⁰² The two instruments—agreed by consensus of 160 countries—were intended to provide clear international standards for intellectual property protection in the digital media environment.²⁰³ President Bill Clinton expressed the belief that the new bill would “extend intellectual protection into the digital era while preserving fair use and limiting infringement liability for providers of basic communication services.”²⁰⁴

The DMCA consists of two key components.²⁰⁵ The first, the anti-circumvention provision outlaws trafficking in all kinds of technology and devices designed to circumvent access-protection or copy-protection measures put in place by copyright owners.²⁰⁶ In other words, it provides legal protection to digital locks that limit access as well as ability to use copyrighted works that employ such measures.²⁰⁷ It also, for the first time, expanded the U.S. copyright law to include an exclusive right to “access.”²⁰⁸

The other major provision, referred to as the Online Copyright Infringement Liability Limitation Act (OCILLA),²⁰⁹ provides

²⁰¹ World Intellectual Property Organization Copyright Treaty, *adopted* Dec. 20, 1996, 36 I.L.M. 65.

²⁰² World Intellectual Property Organization: Performances and Phonograms Treaty, *adopted* Dec. 20, 1996, 36 I.L.M. 76; Stephen E. Blythe, *The U.S. Digital Millennium Copyright Act and The E.U. Copyright Directive: Comparative Impact on Fair Use Rights*, 8 TUL. J. TECH. & INTELL. PROP. 111, 116 (2006).

²⁰³ S. REP. NO. 105-190, at 4–5 (1998).

²⁰⁴ Statement on Congressional Action on Digital Millennium Copyright Legislation, 34 WEEKLY COMP. PRES. DOC. 2034 (Oct. 12, 1998).

²⁰⁵ See 17 U.S.C.A. § 1201 (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/07/12) (anti-circumvention provision); 17 U.S.C.A. § 512 (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/07/12) (providing limited liability to online service providers).

²⁰⁶ § 1201(a)(2).

²⁰⁷ See Blythe, *supra* note 202, at 117–18 (discussing legal protections of the anti-circumvention section).

²⁰⁸ See S. REP. NO. 105-190, at 12 (explaining that the statute provides a right of access in addition to traditional copyright rights).

²⁰⁹ Digital Millennium Copyright Act, Pub. L. No. 105-304, § 201, 112 Stat.

limitations to online copyright liability for Online Service Providers (OSP).²¹⁰ This provision, better known as the DMCA's "safe harbor,"²¹¹ seeks to promote online innovation by providing greater clarification for OSPs' liability resulting from third party infringements.²¹² The DMCA safe harbor provision also comprehended the need for soliciting cooperation from service providers in the fight against widespread digital piracy.²¹³ It achieved this objective by purporting to reach a balance that "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."²¹⁴

B. General Contour of the DMCA Safe Harbor

The second title of the Digital Millennium Copyright Act, now codified as § 512 of the Copyright Act, provides safe harbors against all claims of copyright liability – including "direct, vicarious and contributory infringement."²¹⁵ The safe harbor provision identifies four distinct categories of problematic online activities that might be able to qualify for privilege: (a) maintaining transitory network communications, (b) performing a system caching function, (c) storing information on systems or networks at the direction of users, and (d) offering information location tools.²¹⁶ Online businesses may also be subject to the safe harbor provisions if they perform functions specified in § 512.²¹⁷

2860, 2681 (1998) (codified as amended at 17 U.S.C.A § 512).

²¹⁰ § 512(a)–(d). "[T]he term 'service provider' means a provider of online services or network access, or the operator of facilities therefor," including "an entity offering the transmission, routing, or providing of connections for digital online communications." *Id.* §§ 512(k)(1)(A), (B).

²¹¹ Wendy Seltzer, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment*, 24 HARV. J.L. & TECH. 171, 201–02 (2010).

²¹² *Id.*; S. REP. NO. 105-190, at 2. The Committee on the Judiciary stated, "without clarification of their liability, service providers may hesitate to make the necessary investment in the expansion of the speed and capacity of the Internet." *Id.* at 8.

²¹³ *Id.* at 8–9.

²¹⁴ *Id.* at 20.

²¹⁵ *Id.* at 43; Digital Millennium Copyright Act, Pub. L. No. 105-304, §§ 201, 112 Stat. 2860, 2681 (1998) (codified as amended at 17 U.S.C.A § 512).

²¹⁶ 17 U.S.C.A §§ 512 (a)–(d) (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/07/12).

²¹⁷ See Ginsburg, *supra* note 64, at 579, 591–94 (discussing the application of § 512(c) to online businesses).

The protection afforded by § 512 generally exempts eligible service providers from almost all respects of copyright liability, but it does not create a complete exemption.²¹⁸ A service provider that qualifies for protection will be immune from monetary damages but may still be subject to limited injunctive and other equitable relief within the scope of subsection 512(j).²¹⁹

1. Threshold Requirements

While § 512 promises immunity from infringement liability for service providers of the types discussed above, it does so by demanding a calculated trade-off from eligible providers.²²⁰ For a service provider to qualify for the limitation of liability under § 512, it must satisfy two threshold conditions set forth in subsection 512(i).²²¹ First, a service provider must implement and notify users of a policy of terminating services to subscribers who are repeat online infringers;²²² second, a service provider must accommodate technical protection measures that copyright holders employ to aid in hindering and detecting copyright infringement.²²³

a. Repeat Infringer Termination Policy (R.I.P.)

The DMCA's termination policy threshold is a topic subject to much debate.²²⁴ Copyright owners argue that OSPs must at least implement an effective system that prevents recidivists from continuing use of their service.²²⁵ However, this proposal threatens to place OSPs under a substantial burden of having to investigate and track the behavior of their subscribers.²²⁶ To make the matter more complicated, both the statutory language and legislative history are equally opaque as to what kind of

²¹⁸ § 512 (a)–(d), (j).

²¹⁹ S. REP. NO. 105-190, at 40–41 (explaining that service providers may still be subject to injunctive relief).

²²⁰ § 512 (i).

²²¹ *Id.*

²²² *Id.* § 512(i)(1)(A).

²²³ *Id.* § 512(i)(1)(B).

²²⁴ *See* Perfect 10, Inc. v. CCBill LLC (*CCBill*), 488 F.3d 1102, 1109–10 (9th Cir. 2007) (discussing the court's interpretation of the threshold policy and the copyright holder's subsequent argument).

²²⁵ *E.g., id.* at 1110.

²²⁶ *See id.* at 1111 (“To identify and terminate repeat infringers, a service provider need not affirmatively police its users for evidence of repeat infringement.”).

subscriber would qualify as a “repeat” or “flagrant” infringer.²²⁷ Apparently concerned that the termination-policy requirement might undermine the core principle of § 512(m), Congress issued an instruction that OSPs’ obligation in implementing this policy would not require them to commit any sleuthing task or make difficult judgments as to the infringing nature of conduct.²²⁸

In addition, the text of the DMCA does not explicitly explain how this measure is to be “reasonably implemented.”²²⁹ Nonetheless, the Ninth Circuit in *CCBill* suggested that this requirement is merely a part of a “working notification system,” and that “an implementation is reasonable if, under ‘appropriate circumstances,’ the service provider terminates users who repeatedly or blatantly infringe copyright.”²³⁰ Many courts have also declined to accept various interpretations from plaintiffs that this threshold provision requires OSPs to act like full-blown copyright police and effectively prevent recidivists from returning to the service.²³¹ On the contrary, some courts have held that a determination of whether there is a failure to implement an infringement policy requires a showing that OSPs have actual knowledge of the “user’s blatant, repeat infringement of a willful and commercial nature.”²³² In other words, these courts suggest

²²⁷ “[T]he DMCA does not define ‘repeat infringer’”. Annemarie Bridy, *Is Online Copyright Enforcement Scalable?*, 13 VAND. J. ENT. & TECH. L. 695, 728 (2011). However, the legislative history defines repeat infringers as those “who repeatedly or flagrantly abuse their access to the Internet through disrespect for the intellectual property rights of others,” S. REP. NO. 105-190, at 52 (1998). This definition suggests that OSPs should take steps to prevent any repeat infringers from using their network, even though their prior conduct may have occurred elsewhere.

²²⁸ S. REP. NO. 105-190, at 52.

²²⁹ 17 U.S.C.A §§ 512 (a)–(d) (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/07/12).

²³⁰ *CCBill*, 488 F.3d at 1109 (The court held that “a service provider ‘implements’ a policy if it has a working notification system, a procedure for dealing with DMCA-compliant notifications, and if it does not actively prevent copyright owners from collecting information needed to issue such notifications.”).

²³¹ See *Corbis Corp.*, 351 F. Supp. 2d 1090, 1102 (W.D. Wash. 2004) (holding that the issue of reasonable implementation is whether “the service provider nonetheless still tolerates flagrant or blatant copyright infringement by its users”); *Io Grp.*, 586 F. Supp. 2d 1132, 1144 (N.D. Cal. 2008) (holding that simply because “a rogue user might reappear under a different user name and identity does not raise a genuine fact issue as to the implementation of [a] policy”).

²³² See, e.g., *Corbis Corp.*, 351 F. Supp. 2d at 1104 (discussing the court’s view on actual knowledge with respect to infringement policies); *Capitol Records*, 821 F. Supp. 2d 627, 638 (S.D.N.Y. 2011) (“While knowledge is not an

that a repeat infringer termination policy should be something that deals with willful infringement—thereby distinguishing between blatant infringers and casual users who inadvertently violate some of the content owner’s exclusive rights for personal enjoyment.²³³

In any case, the ambiguity of the repeat infringer termination requirement is likely to create extra burdens to small OSPs who lack wealth and resources to fully implement the § 512 safe harbor provision.²³⁴ Courts usually adopt a rule of thumb to deal with the indefinite nature of this threshold requirement by showing propensity to award safe harbor protection if an OSP goes to extra lengths to protect copyright.²³⁵

In a recent DMCA dispute, *Flava Works, Inc. v. Gunter*, the Northern District Court of Illinois held that the defendant operator of the “myVidster” service failed to implement a repeat infringer policy, since “[b]eyond his mechanical response to the notices, [the defendant] refuses to concern himself with copyright protection.”²³⁶ The *Flava Works* court acknowledged that the DMCA does not require OSPs to “police their sites for infringement.”²³⁷ However, the court noted that OSPs “are required to investigate and respond to notices of infringement—with respect to content *and* repeat infringers.”²³⁸

One of the most well-known R.I.P. measures is YouTube’s “three strikes” policy (or, more formally, “graduated response”

element of copyright infringement, it is relevant to [an OSP’s] decision whether appropriate circumstances exist to terminate a user’s account.”).

²³³ See *Capitol Records*, 821 F. Supp. 2d at 638 (“There is a difference between [blatant infringers] who know they lack authorization and nevertheless upload content to the internet for the world to experience or copy, and [those] users who download content for their personal use and are otherwise oblivious to the copyrights of others.”).

²³⁴ Mark A. Lemley, *Protect Innovators, Not Copyright Lawyers*, NAT’L L.J. (Oct. 19, 2011), *available* at <http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202519418520&slreturn=1>.

²³⁵ Eric Goldman, *Catching Up on 4 Months of Online Copyright Cases*, TECHNOLOGY & MARKETING LAW BLOG (Aug. 12, 2011, 09:29 AM), http://blog.ericgoldman.org/archives/2011/08/catching_up_on.htm; *In re Aimster*, 334 F.3d 643, 655 (7th Cir. 2003) (“The common element of [the DMCA’s] safe harbors is that the service provider must do what it can reasonably be asked to do to prevent the use of its service by ‘repeat infringers.’”).

²³⁶ *Flava Works, Inc. v. Gunter*, No. 10 C 6517, 2011 WL 3205399, at *10 (N.D. Ill. July 27, 2011).

²³⁷ *Id.*

²³⁸ *Id.*

approach).²³⁹ The three-strike approach terminates a user after three complaints, represented by DMCA-compliant notices, are received.²⁴⁰ The District Court in *Viacom International, Inc. v. YouTube, Inc.* found that YouTube's three-strike measure met the requirements of an acceptable repeat infringer measure.²⁴¹ The popularity of the "three-strikes" approach and its progeny raise an important question of whether a user or subscriber can be automatically turned into a repeat infringer if DMCA takedown notices were repeatedly issued against his or her actions.²⁴² However, the *Viacom* court opined that takedown notices themselves are not evidence of blatant infringement since the users could not be certain that they had downloaded infringing content.²⁴³

b. Standard Technical Measures

"Standard technical measures" refer to technology that is used to protect and help identify copyrighted works.²⁴⁴ For the most part, a service provider only has a passive obligation to implement this technology.²⁴⁵ The DMCA only requires that an OSP "accommodates and does not interfere with" how such technology operates.²⁴⁶

"Although there is currently no [widely-accepted] consensus on

²³⁹ *Viacom Int'l, Inc. v. YouTube, Inc. (Viacom)*, 718 F. Supp. 2d 514, 527–28 (S.D.N.Y. 2010), *aff'd in part, vacated in part, remanded by* 676 F.3d 19 (2d Cir. 2012).

²⁴⁰ *Id. But see* Corynne McSherry, *YouTube Sends Users to Copyright School: Will Content Owners Have to Go, Too?*, ELECTRONIC FRONTIER FOUNDATION (Apr. 15, 2011), <http://www.eff.org/deeplinks/2011/04/youtube-sends-users-copyright-school-will-content> (describing YouTube's announced plan of departing from a graduated response policy to a more user-centric approach of providing copyright education).

²⁴¹ *See Viacom*, 718 F. Supp. 2d at 527–28 (explaining why YouTube's policy was reasonably implemented).

²⁴² *See* Amanda Harmon Cooley, *A Contractual Deterrence Strategy for User-Generated Copyright Infringement and Subsequent Service Provider Litigation*, 64 SMU L. REV. 691, 698–99, 726 (2011) (discussing repeat infringement under 17 U.S.C. § 512(i), in conjunction with Youtube's three-strike policy).

²⁴³ *Viacom*, 718 F. Supp. 2d at 528.

²⁴⁴ 17 U.S.C.A. § 512(i)(2) (West, Westlaw current through P.L. 112-207 (excluding P.L. 112-206) approved 12/07/12).

²⁴⁵ *See* Jennifer Bretan, *Harboring Doubts About the Efficacy of § 512 Immunity Under the DMCA*, 18 BERKELEY TECH. L.J. 43, 51 (2003) (explaining that although a more active requirement may be implied, there is no affirmative requirement).

²⁴⁶ § 512(i)(1)(B).

the application of this technology, all major right holders” rely heavily on it to protect their intellectual assets online.²⁴⁷ “[D]igital copyright enforcement of audio, visual and audiovisual works depends on the application of digital ‘fingerprints’ of those works.”²⁴⁸ Congress envisioned that mandatory implementation of some definitive technology would “be the solution to many of the issues facing copyright owners and service providers in this digital age.”²⁴⁹ But the requirement that these technologies be developed and adopted in accordance with an “open, fair, voluntary, [and] multi-industry standards process,”²⁵⁰ makes it unlikely that fingerprinting technology will qualify as “standard technical measure” anytime soon.²⁵¹

2. Statutory Notice-and-Takedown Safe Harbors

The DMCA safe harbors provide different types of immunity depending on the type of functions performed by service providers.²⁵² The scope of exemption is broadest in the case of service providers that “are acting as mere conduits for information” under 17 U.S.C.A § 512(a).²⁵³ However, for service providers of a type specified in 17 U.S.C.A § 512(c), content hosting providers, and 17 U.S.C.A § 512(d), information location tools providers, immunity from copyright liability is contingent on the implementation of the so-called notice-and-takedown procedure.²⁵⁴ Thus, a provider who hosts material pursuant to a subscribers’ behest is required to designate a registered agent who receives and processes notices of claimed infringement.²⁵⁵ Upon receipt of a notice which meets the requirements of 17 U.S.C.A. § 512(c)(3), a service provider must then “respond[] expeditiously to remove, or disable access to, the material that is

²⁴⁷ Lauren G. Gallo, *The (Im)possibility of “Standard Technical Measures” for UGC Websites*, 34 COLUM. J.L. & ARTS 283, 285–86 (2011).

²⁴⁸ *Id.* at 284–85.

²⁴⁹ S. REP. NO. 105-190, at 51–52 (1998).

²⁵⁰ § 512(i)(2)(A).

²⁵¹ Gallo, *supra* note 247, at 286.

²⁵² *See* Bretan, *supra* note 245, at 47–48 (discussing the applicability of different safe harbor provisions depending on a service provider’s functions).

²⁵³ *See id.* at 48–50 (indicating that service providers performing a conduit function are immunized while the other three functions have more limited protection).

²⁵⁴ *Id.* at 50.

²⁵⁵ 17 U.S.C.A. § 512(c)(2) (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/7/12).

claimed to be infringing.”²⁵⁶ The DMCA also protects a service provider from liability which may arise on account of its removal of materials in a good faith response to a proper notice – subject to an obligation to take responsible steps to notify the interested subscriber who would then have an opportunity to submit a counter notification under 17 U.S.C.A. § 512(g)(3).²⁵⁷

IV. KNOWLEDGE STANDARD UNDER NOTICE & TAKE DOWN SYSTEM OF § 512(C)

The legal standard for determining whether a service provider has knowledge of copyright infringement is the core component of 17 U.S.C.A § 512(c).²⁵⁸ In general, a service provider seeking protection from the § 512(c) safe harbor must show that it (1) “does not have actual knowledge that the material or an activity using the material on the system or network is infringing,” and, absent such actual knowledge, (2) “is not aware of facts or circumstances from which infringing activity is apparent.”²⁵⁹ Upon possession of such knowledge, a service provider wishing to benefit from the limitation of liability under 17 U.S.C.A § 512(c) must “act[] expeditiously to remove, or disable access to, the [infringing] material” residing on its system or network.²⁶⁰

Because the question of whether there is an infringement of copyright can be a difficult one, it is not likely that Congress would expect OSPs to engage themselves in determining the legality of a given user’s activity.²⁶¹ On one hand, the infringing nature of a particular file or content may be obscure to a content-hosting OSP because the underlying infringing activity associated with such content may have occurred elsewhere.²⁶² On the other hand, new innovations for the online distribution of

²⁵⁶ *Id.* § 512(c)(1)(C).

²⁵⁷ *Id.* § 512(g)(1)–(3).

²⁵⁸ *Id.* § 512(c)(1).

²⁵⁹ *Id.* § 512(c)(1)(A)(i)–(ii).

²⁶⁰ *Id.* § 512(c)(1)(A)(iii).

²⁶¹ See Lee C. Milstein, *Avoiding Legal Pitfalls on User-Generated Content Sites*, 11 J. INTERNET L. 3, 6 (2007) (indicating the separation between the policing function, which is to be conducted by copyright owners, and the enforcement of that policing, which is to be conducted by OSPs).

²⁶² S. REP. NO. 105-190, at 44 (1998). The legislative history clarifies that the term “activity” in the context of DMCA’s safe harbor refers to an “activity using the material . . . that is occurring at the site on the provider’s system or network at which the material resides, regardless of whether copyright infringement is technically deemed to occur at that site or at the location where the material is received.” *Id.*

content have ruled out the possibility that an average OSP may be able to discern the nature of use and specific rights concerned with availability of particular content.²⁶³

In any case, it is a common understanding that knowledge requirements under § 512(c) serve only as indicators of whether an OSP is qualified to receive the benefits of the DMCA's safe harbors.²⁶⁴ It is *non sequitur*, however, to conclude that any disqualifying provider will inevitably be liable for the infringing conduct of others.²⁶⁵ As the Committee's report reveals, an entity that meets the knowledge standard of the DMCA and refuses to act on that knowledge merely forfeits its right to safe harbors under § 512(c).²⁶⁶

A. *Independent Knowledge Standard of the DMCA*

Although § 512 of the DMCA emits the air of straightforwardness of a notice-central copyright safe-harbor regime, it actually provides far less certainty for OSPs in assessing their risks of being liable as secondary infringers.²⁶⁷ On one hand, the general contour of § 512 suggests that a service provider has no burden or duty to prevent or anticipate infringement beyond promptly and expeditiously responding to a proper notice issued by the copyright holder by blocking access to infringing material.²⁶⁸ On the other hand, there is nothing in the text of § 512(c) that explicitly exempts an OSP from secondary liability should it fail to expeditiously remove or block infringing materials – if it came to possess certain “knowledge” or

²⁶³ The legislative history provides an example: “[T]he activity at an online site offering audio or video may be unauthorized public performance of a musical composition, a sound recording, or an audio-visual work, rather than (or in addition to) the creation of an unauthorized copy of any of these works.” *Id.*

²⁶⁴ Chang, *supra* note 31, at 196–97.

²⁶⁵ See S. REP. NO. 105–190, at 19 (explaining a disconnect between safe harbor qualification and the possibility of actual infringement activity).

²⁶⁶ *Id.* at 44; H.R. REP. NO. 105–551, pt. 2, at 57 (1998).

²⁶⁷ See Chang, *supra* note 31, at 197–98 (“[A]lthough Congress stated that pirate directories ‘are obviously infringing’ . . . [the cases interpreting the statute] leave copyright holders doubting whether it is ever possible to establish the OSP’s apparent knowledge under the red flag test”).

²⁶⁸ Subsection 512(m)(1) provides that “[n]othing in this section shall be construed to condition the applicability of subsections (a) through (d) on . . . a service provider monitoring its service or affirmatively seeking facts indicating infringing activity.” 17 U.S.C.A. § 512(m)(1) (West, Westlaw through P.L. 112-207 approved 12/07/12).

“awareness” of the same through a less specific source of information than the copyright holders’ DMCA-compliant notice.²⁶⁹ Indeed, as a safe harbor against secondary liability claims, it seems sensible to read the DMCA as providing a way out for OSPs by removing or disabling content expeditiously in two circumstances: (1) when the elements of common law contributory infringement or vicarious liability are met, or (2) upon receipt of a valid DMCA notification.²⁷⁰

One of the problems of this interpretation is that it requires the drafters of the DMCA to adopt a knowledge standard that is substantially parallel to the common law requirements to hold an OSP liable as a contributory infringer.²⁷¹ However, as we have seen in the previous section, the common law knowledge standard under the secondary liability doctrine is an ever-changing and expanding area of jurisprudence.²⁷² In *Grokster*, the Supreme Court went further as to adopt a new tort for inducement of copyright infringement.²⁷³ It is therefore doubtful that a statutory safe harbor, enacted in 1998, would ever encompass – let alone parallel – the ever expanding knowledge theory under common law tort.²⁷⁴ Congress’ awareness of this apparent loophole is evident by its observation that:

Most [cases] have approached the issue [of service provider liability] from the standpoint of contributory and vicarious

²⁶⁹ *Id.* § 512(d)(3). Professor R. Anthony Reese observed that the conditions for DMCA eligibility and the elements of common law contributory liability are closely parallel such that, in some cases, a copyright plaintiff may be allowed to disqualify an OSP from the safe harbor and pursue secondary liability claims. *See Reese, supra* note 16, at 442.

²⁷⁰ *See id.* at 442–43 (describing the common law and statutory approaches as applied to OSPs’ liability).

²⁷¹ *See id.* (“[T]he conditions that an OSP must meet in order to qualify for these safe harbors closely parallel the elements of common law contributory infringement and vicarious liability claims . . .”).

²⁷² *See supra* notes 193-96 and accompanying text. For example, courts since *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 264 (9th Cir. 1996), have done away with the notion that an assisting party needs to be aware of the identity of the direct infringer in order to be held contributorily liable for the latter’s conduct.

²⁷³ *Grokster I*, 545 U.S. 913, 941 (2005).

²⁷⁴ Mark Lemley suggests that while courts have been augmenting the common law doctrine of contributory and vicarious liability, a plain reading of the statute indicates that congress intend § 512 to shield OSPs from those expanded torts. However, the fact that the statute sets out what were commonly understood in 1998 to be the elements of a vicarious infringement claim only serves to complicate the matter further. Lemley, *supra* note 16, at 104 n.23.

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.²⁷⁵

It is also worth remarking that, despite ambivalence in the text of § 512(c) and (d), the legislative history does not make any allusion to the common law standard of knowledge when it elaborates on the scope and meaning of subsections (c)(1)(A)(i) and (c)(1)(A)(ii).²⁷⁶ Common sense counsels us that the whole scheme of the notice-and-takedown regime would crumble if copyright owners could easily forego the trouble of adhering to § 512(c)’s notification protocol and adopt some easier standard of knowledge to pin down an OSP.²⁷⁷ The notice-centrality nature of the DMCA thus strongly argues against the parallel application of the knowledge standard from common law secondary liability jurisprudence.²⁷⁸ This issue will be further discussed in the next section.²⁷⁹

Furthermore, it has long been argued, as a matter of policy, that holding the DMCA’s requirements as parallel to elements of secondary liability would, in effect, exclude contributory and vicarious liability from the scope of § 512(c)’s safe harbors.²⁸⁰ In other words, this co-extensive approach of interpreting the DMCA would lead to a paradoxical conclusion – for it suggests that § 512 may not provide safe harbors for any liability other

²⁷⁵ S. REP. NO. 105-190, at 19 (1998); H.R. REP. NO. 105-551, pt. 1, at 25 (1998) (noting that the DMCA’s “standard differs from existing law, under which a defendant may be liable for contributory infringement if it knows *or should have known* that material was infringing”).

²⁷⁶ S. REP. NO. 105-190, at 40–41; H.R. REP. NO. 105-551, pt. 2, at 53–54. *Cf.* Reese, *supra* note 16, at 438 (arguing that the DMCA indeed mirrors the common law principle of secondary liability in determining whether an OSP qualifies for a safe harbor, but that it modifies those principles by requiring greater knowledge on the part of the OSP).

²⁷⁷ See Edward Lee, *Decoding the DMCA Safe Harbors*, 32 COLUM. J.L. & ARTS 233, 253 (2009) (“A low standard of knowledge would invite constant litigation against [OSPs] . . .”).

²⁷⁸ See *id.* (“Requiring a high level of proof to establish that an [OSP] was ‘aware of facts from which infringing activity is apparent’ serves the purpose of a safe harbor.”).

²⁷⁹ See *infra* Part B.

²⁸⁰ See Lee, *supra* note 277, at 240–43 (arguing that the statutory text of the DMCA is not the same as the traditional vicarious liability standard); *cf.* Lemley, *supra* note 16, at 114 (contending that § 512(c) may contain “a gaping loophole,” as the text does not explicitly provide protection for “any intermediary who is engaged in conduct that the law at that time defined as vicarious infringement”).

than direct infringement.²⁸¹ The consequence of this interpretation is that an OSP would be immediately disqualified from § 512(c)'s shelter as soon as the service provider's operation satisfies all the criteria necessary to hold it contributorily or vicariously liable under the common law doctrine.²⁸² Nevertheless, given Congress' clear mandate in three different reports that the DMCA was intended to afford protection to qualifying service providers against "all monetary relief for direct, vicarious and contributory infringement," it is highly improbable that Congress intended to make § 512(c) parallel in structure to the requirements of these common law liabilities.²⁸³

In sum, while it is tempting to regard the DMCA's safe harbor regime as being parallel to common law standard of contributory and vicarious infringement doctrine, the legislative history – and, as we shall see, case law – are quite clear that § 512(c) employs a standard of knowledge different from that of common law claims.²⁸⁴ It is thus only sensible – given the whole structure of § 512 – for a knowledge standard to be applied it must be one that is consistent with the principle that an OSP is entitled to safe harbor protection without having to take part in the investigation or confirmation of claimed infringement.²⁸⁵

B. Notice-Centrality Aspect of Actual Knowledge

Courts that have addressed the application of § 512(c) safe harbor have commonly agreed that notification issued pursuant to the requirement of subsection 512(c)(3) is the most important type of knowledge that will trigger a service provider's duty to take down infringing material.²⁸⁶ Hence, the plaintiff's failure to supply notice of claimed infringement prior to suit can have a devastating effect on his ability to impose actual knowledge on a

²⁸¹ Lee, *supra* note 277, at 243–44.

²⁸² *Id.* at 244.

²⁸³ H.R. REP. NO. 105-796, at 73 (1998) (Conf. Rep.); S. REP. NO. 105-190, at 20 (1998); H.R. REP. NO. 105-551, pt. 2, at 50 (1998). This issue is finally addressed in the water-shed appellate decision in *UMG III*, in which the Ninth Circuit rejected the parallel-requirement theory between § 512 and the common law standard of vicarious liability. *UMG III*, 667 F.3d 1022, 1042 (9th Cir. 2011); Lee, *supra* note 277, at 237.

²⁸⁴ S. REP. NO. 105-190, at 19; H.R. REP. NO. 105-551, pt. 1, at 25.

²⁸⁵ 17 U.S.C.A. § 512(m) (West, Westlaw through P.L. 112-207 approved 12/07/12).

²⁸⁶ *Corbis Corp.*, 351 F. Supp. 2d 1090, 1107 (W.D. Wash. 2004).

defendant.²⁸⁷ In fact, attempts to establish “actual knowledge” from evidence other than valid DMCA notifications have usually floundered.²⁸⁸ Courts have held these types of evidence to be no more than endeavors to establish “general awareness” which is not sufficient to replace actual and specific knowledge from a service of proper notice.²⁸⁹ In *Viacom*, after a lengthy review of legislative history, the New York District Court concluded that the phrase “actual knowledge . . . describe[s] knowledge of specific and identifiable infringements of particular individual items. Mere knowledge of prevalence of such activity in general is not enough.”²⁹⁰

Certain requirements regarding the form and content of a valid notification also reflect Congressional intent that the knowledge standard under the DMCA should be different from notice that might establish a contributory infringement cause of action.²⁹¹ The goal of the statutory notice is to provide the service provider with sufficient information to locate and examine the allegedly infringing material expeditiously and without undue investigation.²⁹² To achieve this goal, the DMCA requires that the content of the notification under § 512(c)(3) substantially comply with the overall requirements under that subsection.²⁹³ This “substantial compliance” is not a particularly stringent standard.²⁹⁴ The DMCA in fact allows some trivial information to

²⁸⁷ See, e.g., *Io Grp.*, 586 F. Supp. 2d 1132, 1148 (N.D. Cal. 2008) (“It is undisputed that, before it filed the instant action, plaintiff provided no notice to Veoh of any claimed copyright infringement. Thus, there is no question on the record presented that Veoh lacked actual knowledge of the alleged infringing activity at issue.”).

²⁸⁸ See, e.g., *Corbis Corp.*, 351 F. Supp. 2d at 1108 (“[plaintiff’s] decision to forego the DMCA notice provisions . . . stripped it of the most powerful evidence of a service provider’s knowledge – actual notice of infringement from the copyright holder.”).

²⁸⁹ See, e.g., *id.* at 1107–08 (“The issue is not whether [the defendant] had a general awareness that a particular type of item may be easily infringed. The issue is whether [the defendant] actually knew that specific . . . vendors were selling items that infringed [the plaintiff’s] copyrights.”); *Capitol Records*, 821 F. Supp. 2d 627, 644 (S.D.N.Y. 2011) (“General awareness of rampant infringement is not enough to disqualify a service provider of protection.”).

²⁹⁰ *Viacom*, 718 F. Supp. 2d 514, 519–23 (S.D.N.Y. 2010).

²⁹¹ Reese, *supra* note 16, at 437.

²⁹² 17 U.S.C.A. § 512(c)(3)(A)(iii) (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/7/12).

²⁹³ *Id.* § 512(c)(3)(A); S. REP. NO. 105-190, at 46 (1998) (“The standard against which a notification is to be judged is one of substantial compliance.”).

²⁹⁴ See S. REP. NO. 105-190, at 47 (holding that certain technical errors do not disqualify service providers and copyright owners from the protections of the

be omitted from a DMCA notice without rendering it invalid.²⁹⁵ The notice served, thus, needs only provide substantially enough information to satisfy this important function.²⁹⁶

Additionally, a qualified DMCA notice must also provide information regarding claimed infringement in an efficient manner.²⁹⁷ In *Perfect 10, Inc. v. CCBill LLC*, the Ninth Circuit interpreted the phrase “a written communication” in § 512(c)(3)(A) as requiring that a proper DMCA notice exist in a single written communication.²⁹⁸ The *CCBill* court rejected the plaintiff’s argument that a combination of three sets of documents, only one of which was signed under penalty of perjury, could constitute effective notice under the DMCA, since “[p]ermitting a copyright holder to cobble together adequate notice from separately defective notices also unduly burdens service providers.”²⁹⁹

Courts’ close adherence to the principle of notice-centrality raises the question as to whether “actual knowledge” could ever be satisfied other than through service of proper notices.³⁰⁰ Both the legislative history and the textual language of the DMCA’s safe harbor itself, however, lend support to the conclusion that it is highly improbable for a plaintiff to prove actual knowledge or even awareness of infringement if he chooses to forego the notice in the first place.³⁰¹ Indeed, it is an explicit statement of Congress that “neither actual knowledge nor awareness of a red flag may be imputed to a service provider” if information signifying such knowledge does not comply with the notice provision of subsection 512(c)(3).³⁰² Professor Nimmer, copyright law’s leading

statute).

²⁹⁵ *Id.*

²⁹⁶ *See id.* (providing examples of technical errors that would not invalidate the notice).

²⁹⁷ *Id.*

²⁹⁸ 488 F.3d 1102, 1112–13 (9th Cir. 2007).

²⁹⁹ *Id.*

³⁰⁰ *See* 17 U.S.C.A. § 512(c) (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/7/12) (focusing on the importance of notification to establish actual knowledge).

³⁰¹ S. REP. NO. 105-190, at 45 (1998); § 512(c)(3)(B)(i) (“[A] notification from a copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.”).

³⁰² S. REP. NO. 105-190, at 45.

commentator, observes that “the structure of OCILLA effectively prevents an owner from ‘lying in the weeds’ by failing to provide notice, and then belatedly claiming that vast damages have accrued in the interim.”³⁰³ Consequently, while the text of § 512 and its legislative history does not explicitly reject other types of evidence, it is not too far-fetched to conclude that a determination of knowledge under the DMCA is largely a matter of whether a copyright holder adheres to the safe harbors’ notification requirements.³⁰⁴

In sum, without the notice-centrality aspect, the DMCA cannot be expected to provide OSPs with an effective and reliable shelter from indirect liability.³⁰⁵ It serves the DMCA’s purpose by effectively divesting service providers of the duty to either initiate an investigation or confirm suspicion pertaining to infringing acts – even in circumstances where a reasonable person may be required to do so.³⁰⁶

Nevertheless, the actual picture of real copyright practice is far different from what the statutory scheme intended.³⁰⁷ Recent case law revealed that OSPs have the propensity to respond to all types of complaints from copyright holders.³⁰⁸ With an overwhelming number of copyright notices served each day, most service providers simply cannot be expected to ferret out DMCA-compliant notices from non-compliant ones.³⁰⁹ Under these

³⁰³ NIMMER & NIMMER, *supra* note 46, at § 12B.04[A][2][c][3] n.43.

³⁰⁴ *See Capitol Records*, 821 F. Supp. 2d 627, 643-44 (S.D.N.Y. 2011) (describing the actual knowledge requirement as disqualifying an entity from using the safe harbor).

³⁰⁵ *See, e.g., id.* at 644–45 (explaining that without notice, the OSP will not be liable for infringing activity, even if a reasonable person would know infringing activity was taking place).

³⁰⁶ *See id.* (holding that while a reasonable person might conclude after some investigation that the links hosted or provided on an OSPs’ site actually lead to infringing copies of a copyrighted work, the DMCA does not place such investigative burdens on a service provider).

³⁰⁷ *See Jason Mazzone, Copyfraud*, 81 N.Y.U. L. REV. 1026, 1035–36 (2006) (explaining that statutory penalties exist for copyright infringement, but protection is not afforded to public domain material and there is also a lack of available redress for misleading copyright attempts on uncopyrightable material).

³⁰⁸ *See Arista Records LLC v. Myxer Inc. (Myxer Inc.)*, 2011 U.S. Dist. LEXIS 109668, at *6–8 (C.D. Cal. Apr. 1, 2011) (exemplifying an OSP’s response where a plaintiff failed to send a valid DMCA notice, but defendant treated all complaints as DMCA notices and promptly removed the infringing files it was able to locate).

³⁰⁹ *See Amit Singhal, An Update to our Search Algorithms*, INSIDE SEARCH (Aug. 10, 2012, 10:30AM), <http://insidesearch.blogspot.de/2012/08/an-update-to>

circumstances, it should not be surprising that abusive notification practices by content owners are ubiquitous.³¹⁰ Some copyright holders misleadingly communicate to service providers and users alike that they own copyrights in public domain material.³¹¹ To aggravate the matter, courts have largely deferred to the notification power of copyright plaintiffs – making the notification power a formidable tool for SLAPP practice and forcing OSPs to err on the side of copyright owners.³¹²

C. Apparent Knowledge or “Red Flag” Test

Another key component to the knowledge standard under § 512(c) is what came to be known as the “red flag” test.³¹³ Absent the primary “actual” knowledge, an OSP may still lose its safe harbor if it is aware of circumstance where infringing activities are apparent.³¹⁴ A determination of whether a red flag test has been met consists of two prongs – subjective and objective considerations.³¹⁵ The first prong requires that there be subjective awareness on the part of a service provider relating to facts and circumstances of infringement.³¹⁶ The second prong, on the other hand, provides us with a test for determining whether such facts and circumstances constitute an impermissible “red flag.”³¹⁷ The legislative reports identify the nature of the test to

our-search-algorithms.html (providing an example of the increased volume of infringement notices sent to a large and influential content provider, and the trouble the provider has in dealing with the high volume).

³¹⁰ See Mazzone, *supra* note 307, at 1029 (“False assertions of copyright are everywhere.”).

³¹¹ *Id.* at 1028 (raising an example of a misleading copyright notice in a pocket version of the U.S. Constitution).

³¹² For example, in *Capital Records, Inc. v. MP3Tunes, LLC*, the District Court held that the plaintiff’s notice has the power to demand removal of material stored in users’ private lockers, and rejected MP3Tunes’ claim that its users had the expectation of privacy in their private lockers. 821 F. Supp. 2d 627, 643 (S.D.N.Y. 2011). The court opined that such users were entitled to use put back procedures under § 512(g) to respond to these copyright notices. *Id.*; 17 U.S.C.A. § 512(g) (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/7/12).

³¹³ S. REP. NO. 105-190, at 44 (1998).

³¹⁴ See 17 U.S.C.A. § 512 (c)(1)(A)(ii) (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/7/12) (stating that without knowledge or awareness of the circumstances, a service provider shall not be liable).

³¹⁵ S. REP. NO. 105-190, at 44.

³¹⁶ *Id.*

³¹⁷ *Id.*

be “whether those facts or circumstances constitute a ‘red flag’—in other words, whether infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances.”³¹⁸

1. The Inherent Paradoxes of the Red Flag Test

The red flag creates voluminous and contentious debates among scholars and courts because it is difficult to ascertain the appropriate standard that courts should apply to such a test.³¹⁹ Congress incorporated apparent knowledge into the DMCA because the actual knowledge standard is a difficult one to meet.³²⁰ If copyright holders fail to comply with § 512’s notice requirements, a cynical online provider may get away from liability simply by ignoring blatant indications of infringement.³²¹ The existence of the red flag test, however, is responsible for much of the DMCA’s interpretational challenges – most importantly because the red flag theory threatens to undermine the integrity of the DMCA’s core principle that no investigative burden should be imposed on any service provider.³²²

a. Apparent Knowledge and Reasonable Person Standard

The reasonable person standard of the objective prong in the red flag test apparently runs against the fundamental principle of § 512, which maintains that a service provider neither needs to monitor its service, nor affirmatively investigate facts indicating infringing activity.³²³ An obvious problem of the reasonable person standard is that it permits courts to adduce evidence from a large scope of factual circumstances for the purpose of establishing the defendant’s knowledge or awareness with regard to infringing activities.³²⁴ Consequently, a combination of apparent knowledge theory and the “reasonable person” standard suggests that an OSP can be disqualified from § 512’s safe harbor based on evidence far less definite in nature when compared with

³¹⁸ *Id.*; H.R. Rep. No. 105-551, pt. 2, at 50 (1998).

³¹⁹ Lee, *supra* note 277, at 234.

³²⁰ *Id.*

³²¹ NIMMER & NIMMER, *supra* note 46, at § 12B.04[A][1].

³²² Lee, *supra* note 277, at 253.

³²³ 17 U.S.C.A. § 512(m) (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/7/12); S. REP. NO. 105-190, at 44.

³²⁴ *See* S. REP. NO. 105-190, at 44 (1998) (describing how facts and circumstances are applied to an objective standard to determine knowledge).

a proper DMCA notice – provided that such evidence would prompt a “reasonable person” to acknowledge that some piratical operation is at hand.³²⁵

Regardless, courts tend to treat this recommendation as though it does not exist.³²⁶ In *Corbis Corp.*, for example, the District Court squarely rejected the reasonable person standard as inapplicable to the analysis of the DMCA’s apparent knowledge.³²⁷ In that case, plaintiff Corbis sought to defeat Amazon.com’s § 512(c) defense by claiming that Amazon was aware of the facts and circumstance from which alleged infringing activity was apparent.³²⁸ Because Corbis never attempted to notify Amazon that zShops vendors were selling images that violated its copyrights, Corbis relied largely on third-party notices in arguing that Amazon must have been aware of the relevant facts and circumstances.³²⁹ Disagreeing with Corbis’ interpretation of § 512(c), the court held that:

In determining whether a service provider is “aware of facts or circumstances from which infringing activity was apparent,” the question is not “what a reasonable person would have deduced given all the circumstances.” Instead, the question is “whether the service provider deliberately proceeded in the face of blatant factors of which it was aware.”³³⁰

The *Corbis* court’s observation is fundamentally correct.³³¹ A reasonable person standard may be a proper tool to determine whether a tortious liability exists when some known legal duty has been neglected.³³² But a service provider, under the entire scheme of the DMCA’s § 512, is understood to bear no such generalized obligation – save the implementation of § 512(i) threshold requirements and a functioning notice-and-takedown

³²⁵ See *id.* at 44–45 (explaining the different knowledge requirements for exclusion from the safe harbor provision and noting the detailed notice requirements under § 512 (c)(3)).

³²⁶ See, e.g., *Capitol Records*, 821 F. Supp. 627, 644 (S.D.N.Y. 2011) (holding that the reasonable person standard cannot be relied upon to place the burden of investigation on the service provider).

³²⁷ *Corbis Corp.*, 351 F. Supp. 2d 1090, 1108 (W.D. Wash. 2004).

³²⁸ *Id.*

³²⁹ *Id.* at 1107–08.

³³⁰ *Id.* at 1108.

³³¹ See *id.* (describing how this analysis is consistent with Congressional intent).

³³² RESTATEMENT (SECOND) OF TORTS: CONDUCT OF A REASONABLE MAN: THE STANDARD §283 (2012).

system.³³³ Nonetheless, it should be noted that the *Corbis* court only rejected the reasonable person standard when it is used to support an argument that some obscure legal duty should be imposed on service providers.³³⁴ There may still be other circumstances where reasonable providers are required to take action in the face of a high probability of infringement instead of turning a blind eye on illegal conducts of their users.³³⁵

b. Proving Red Flag Appears to Be an Insurmountable Task

Setting the reasonable person standard aside, the legislative reports deem it to be an important policy reason that a high standard should be set for a determination of apparent awareness of infringement.³³⁶ Many commentators interpreted Congress's examples of conduct blatant enough to constitute a red flag as clearly pointing out that the apparent knowledge of red flag must come from a *strong indication* of the infringing nature of the activity.³³⁷ However, as it turns out, nobody has hitherto been able to explain the precise nature or scope of the appropriate red flag standard.³³⁸ Indeed, when it comes to a discussion of the red flag test, the existing body of our DMCA jurisprudence is nothing short of amazing guesswork.³³⁹

The courts certainly are not the only ones to blame. The legislative history of the DMCA appears highly inconsistent when it comes to how the red flag test should be applied.³⁴⁰ Throughout the discussion of apparent knowledge, the legislative

³³³ See *Corbis Corp.*, 351 F. Supp. 2d at 1106–07 (explaining that in order to escape liability, the defendant must show (1) that it lacked actual or apparent knowledge of the infringing activity, (2) it did not receive a direct financial benefit from the infringing activity, and (3) it acted expeditiously to remove the infringing material).

³³⁴ *Id.* at 1107–08.

³³⁵ See Reese, *supra* note 16, at 434–35 (discussing the Congressional intention behind the knowledge requirements).

³³⁶ See NIMMER & NIMMER, *supra* note 46, at §12B.04[A][1] (noting that the “red flag” may need to display a very bloody hue indeed before it can trigger the service provider’s obligation to intervene with infringing activities).

³³⁷ *Id.*; see Reese, *supra* note 16, at 434–35 (A provider may be deprived of safe harbor only if such provider “has seen a ‘red flag’ of obvious infringement.”); Ginsburg, *supra* note 64, at 596 (explaining that the high knowledge standard “suggests the [red] flag may need to be an immense crimson banner before the service provider’s obligation to intervene comes into play”).

³³⁸ Lee, *supra* note 277, at 234.

³³⁹ *Id.*

³⁴⁰ S. REP. NO. 105-551, at 57–58 (1998).

reports repeatedly negate the possibility that an OSP may need to make discriminating judgment regarding the legality of suspected materials.³⁴¹ At the same time, Congress expresses confidence that there should be ample instances where rogue websites can be “obviously pirate” such that a brief encounter with them is all that is needed to have encountered a red flag.³⁴² In this regard, the contradictory nature between the DMCA’s underlying principle and apparent knowledge standard makes it doubtful as to whether there can ever be a red flag.³⁴³

i. General Judicial Disregard of Legislative Recommendation

Congress apparently refrained from elaborating on the precise nature of the apparent knowledge standard.³⁴⁴ Instead, Congress opted for an easy solution by suggesting various examples that it believes would best illustrate the infringing nature of third party’s conduct to the OSP.³⁴⁵ These involve the use of obvious words of infringement and inducement “such as ‘pirate,’ ‘bootleg,’ or slang terms in their URL [uniform resource locator] and header information”³⁴⁶ According to the Senate Report, these terms should by themselves, activate a red flag “[b]ecause the infringing nature of such sites would be apparent from even a brief and casual viewing”³⁴⁷ The central premise of this recommendation is based on what Congress calls a “common-sense” approach in which a presumption against online providers’ general obligation of making discriminatory judgment may be overcome, should an OSP encounter an Internet site which is “obviously pirate.”³⁴⁸ Congress, however, failed to take into account the varying context of how a copyrighted material is now distributed or made available on the Internet.³⁴⁹

³⁴¹ *See id.* (explaining what the § 512(d) test requires when online editors and catalogers encounter a red-flag website).

³⁴² *Id.*

³⁴³ *See id.* (stating that ordinarily, OSP’s are not required to make determinations about the existence of a red-flag).

³⁴⁴ *See id.* at 53 (describing how the apparent knowledge standard may be met).

³⁴⁵ *Id.* at 53–54.

³⁴⁶ S. REP. NO. 105-551 at 58.

³⁴⁷ *Id.*

³⁴⁸ *Id.*

³⁴⁹ *See Ginsburg, supra* note 64, at 594 (explaining that Congress’ use of the term “service provider” necessarily encompasses a broader range of Internet entities than legislators had in mind).

In the Ninth Circuit's 2007 decision, *CCBill*, the court pointed out the logical flaw of this red flag indicating measure and declined to hold that the defendant CCBill was aware of red flags simply because it provided service to a site with suggestive URLs such as "illegal.net" and "stolencelebritypics.com."³⁵⁰ The *CCBill* court reasoned that the choice of name for a website, however suggestive of the illicit nature of material posted, may be a result of considerations other than to induce infringement of copyright.³⁵¹ A number of well-known cases have followed the aberrational logic of the *CCBill* court – in defiance of the legislative report's suggestion.³⁵²

More recently, in *Capital Records, Inc. v. MP3Tunes, LLC*, a New York District Court likewise refused to construe terms such as "free," "mp3," or "file-sharing" as tantamount to indications of red flag awareness.³⁵³ In that case, the defendant MP3Tunes, formerly doing business as MP3.com, operated a cloud-based music locker service that allowed users to upload digitized recordings that can be accessed by any device having online connection.³⁵⁴ Users normally uploaded music from their hard drives, but the "Webload" feature also allowed users to upload a music file stored on a third-party server by entering a URL.³⁵⁵ Moreover, MP3Tunes also offers a music search engine service called Sideload.com that lets users find free music on the Internet.³⁵⁶ Sideload's concept is to set up a searchable directory of free music available on the Internet through third party sites.³⁵⁷

The plaintiff EMI argued that MP3Tunes should have been

³⁵⁰ *CCBill*, 488 F.3d 1102, 1114–15 (9th Cir. 2007).

³⁵¹ *Id.* at 1114 ("When a website traffics in pictures that are titillating by nature, describing photographs as 'illegal' or 'stolen' may be an attempt to increase their salacious appeal, rather than an admission that the photographs are actually illegal or stolen.").

³⁵² *UMG Recordings, Inc. v. Veoh Networks, Inc.* (*UMG II*), 665 F.Supp. 2d 1099, 1108 (C.D. Cal. 2009 (citing *CCBill*, 488 F.3d at 114). *See e.g., Io Grp.*, 586 F. Supp. 2d 1132, 1148, 1149 (N.D. Cal. 2008) (rejecting the plaintiff's argument that the absence of mandatory label on sexually explicit materials constitutes a red flag because Veoh should have known that no legitimate producer of sexually explicit material would have omitted the requisite labels on the video clips).

³⁵³ *Capitol Records*, 821 F. Supp. 2d 627, 644 (S.D.N.Y. 2011).

³⁵⁴ *Id.* at 633.

³⁵⁵ *Id.* at 633–34.

³⁵⁶ *Id.* at 634.

³⁵⁷ *Id.*

aware of the fact and circumstance of apparent infringement since the lists of songs compiled on its “Sideload” search engine contained names of popular artists and were gotten from obviously infringing sites compiled on Sideload’s directory.³⁵⁸ MP3Tunes’s executives also used “Sideload” features to obtain songs from the pirate sites.³⁵⁹

The court, commenting along the same line as *CCBill*, held that the terms “free,” “mp3,” or “file-sharing” are “ubiquitous among legitimate sites offering legitimate services.”³⁶⁰ The use of these terms may indicate nothing more than that the sites using them are popular file-sharing sites.³⁶¹ The *MP3Tunes* court then reiterated the well-grounded principle from *CCBill* that no facts or circumstances can constitute a red flag, if *any* investigation on the part of an OSP is required to determine whether material is infringing.³⁶² To make the matter decisive, the court also declined to apply the reasonable person standard to MP3Tunes, reasoning that it would “undermine Congress’s [sic] goal of fostering development and innovation of internet services.”³⁶³

In another recent decision, *Arista Records, LLC v. Myxer Inc.*, the District Court of Central District of California clarified that “there is no caselaw suggesting that ‘a provider’s general awareness of infringement, without more, is enough to preclude application of § 512(c).’”³⁶⁴ In *Myxer Inc.*, the defendant Myxer allowed users to upload songs to be turned into ring tones and categorized available songs as “Most Popular,” “Recent Downloads,” or “Just Shared.”³⁶⁵ The plaintiff, Arista Records, argued that such categorization evinced the required red flag awareness because “Top 40 songs are ‘inevitably copyrighted.’”³⁶⁶ The court observed that Top 40 songs available on the Internet are not obviously infringing because “performers may waive

³⁵⁸ *Id.* at 634, 636.

³⁵⁹ *Capitol Records*, 821 F. Supp. 2d at 635.

³⁶⁰ *Id.* at 644.

³⁶¹ *See id.* (stating that the terms at issue cannot automatically be viewed as hallmarks of sites that endorse copyright infringement and thus are not red-flags).

³⁶² *Id.* (citing *CCBill*, 488 F.3d 1102, 1114 (9th Cir. 2007)) (“[I]f investigation is required to determine whether material is infringing, then those facts and circumstances are not ‘red flags.’”).

³⁶³ *Id.*

³⁶⁴ *Myxer Inc.*, 2011 U.S. Dist. LEXIS 109668, at *80–81 (C.D. Cal. Apr. 1, 2011) (citing *UMG II*, 665 F. Supp. 2d 1099, 1111 (C.D. Cal. 2009)).

³⁶⁵ *Id.* at *85.

³⁶⁶ *Id.* (citing *Grokster I*, 545 U.S. 913, 926 (2005)).

copyright in the hope that it will encourage the playing of their music and create a following that they can convert to customers of their subsequent works.”³⁶⁷ The *Myxer Inc.* court accordingly denied plaintiffs’ motion for summary judgment on the issue of red flag knowledge, concluding that “Myxer’s awareness of popular downloads, recently downloaded music, and just-shared files does not, as a matter of law, establish knowledge of a ‘red flag.’”³⁶⁸

The *Myxer Inc.* court’s opinion is interesting in the sense that it rejects a red flag claim against an OSP who *actually* employed words with infringing connotation to describe the content hosted on its own site.³⁶⁹ The obvious logic of the *Myxer Inc.* court’s holding – as well as similar conclusions from other courts – is that apparent knowledge of infringing circumstance must be based on the manifested infringing nature of a particular work, and not just a derived conclusion based on the place in which the work is available, or the name by which it is described.³⁷⁰

ii. Unavailability of Other Evidence

It is not entirely clear why these aberrations from legislative records have occurred in such a coherent manner among the courts.³⁷¹ But other types of evidence cited by plaintiff copyright holders to support their claims of red flag knowledge did not fare any better than the use of obvious infringing terms.³⁷² For example, in *CCBill*, the Ninth Circuit also rejected the plaintiff’s argument that the defendant CWIE’s hosting of “password-hacking” websites – sites that unlawfully provide users with log-in names and passwords to access other websites – can, by itself, constitute a red flag due to the sites’ obviously infringing nature.³⁷³ The court, however, considered the illicit nature of such sites to be primarily instructing and enabling users “how to engage in an infringing use.”³⁷⁴ In other words, the password-

³⁶⁷ *Id.* at *85.

³⁶⁸ *Id.* at *86.

³⁶⁹ *See id.*

³⁷⁰ *Myxer Inc.*, 2011 U.S. Dist. LEXIS 109668, at *89.

³⁷¹ *See CCBill*, 488 F.3d 1102, 1118 (9th Cir. 2007) (discussing what the legislative history expressly states regarding infringing activities).

³⁷² *See id.* at 1113–14, 1118 (discussing red-flag knowledge in comparison to actions constituting obvious infringing terms).

³⁷³ *Id.* at 1114.

³⁷⁴ *Id.* (quoting *Grokster I*, 545 U.S. 913, 936 (2005)).

hacking sites are merely potential contributory infringers. Their existence alone could tell nothing about the actual infringement committed by people who rely on their service – let alone their own liability.³⁷⁵ According to the court,

[I]n order for a website to qualify as a “red flag” of infringement, it would need to be apparent that the website instructed or enabled users to infringe another’s copyright. . . . We find that the burden of determining whether passwords on a website enabled infringement is not on the service provider.³⁷⁶

The *CCBill* court further explained that such “website[s] could be a hoax, or [their password information] out of date.”³⁷⁷ Moreover, the access codes provided may be freely supplied as a short-term promotion or for other legitimate purposes. In short, “[t]here is simply no way for a service provider to conclude that the passwords enabled infringement without trying the passwords.”³⁷⁸

Despite copyright holders’ unrelenting creative efforts in trying to meet red flag requirements through other evidence, their hitherto lack of success points toward a gloomy realization that courts are likely to refuse a copyright holder’s red flag claim when an OSP adequately follows notice-and-takedown protocols, but the copyright holder failed to notify the defendant with proper DMCA notices.³⁷⁹ Indeed, the text of the DMCA itself forbids a copyright owner from resorting to apparent knowledge when her notices fell short of substantially satisfying the requirements of notice provision.³⁸⁰

³⁷⁵ *See id.* (“Similarly, providing passwords that enable users to illegally access websites with copyrighted content may well amount to contributory infringement.”).

³⁷⁶ *Id.* (citing *Napster II*, 239 F.3d 1004, 1013 (9th Cir. 2001)).

³⁷⁷ *CCBill*, 488 F.3d 1102, 1114 (9th Cir. 2007).

³⁷⁸ *Id.*

³⁷⁹ *See, e.g., id.* at 1114 (“Notice that fails to substantially comply with § 512(c)(3)(B) . . . cannot be deemed to impart such awareness.”); *Wolk v. Kodak Imaging Network, Inc.*, No. 10 Civ. 4135, 2011 U.S. Dist. LEXIS 27541, at *14 (S.D.N.Y. Mar. 17, 2011) (“Without receiving notices identifying and locating each instance of infringement, Photobucket did not have ‘actual knowledge’ of the complained of infringements or ‘aware[ness] of facts or circumstances from which infringing activity is apparent.’”).

³⁸⁰ 17 U.S.C.A. § 512(c)(3)(B)(i) (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/7/12) (“a notification from a copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from

In sum, our recent line of case law appears to agree on a remarkable conclusion: that apparent knowledge can never be found unless a plaintiff produces evidence which can demonstrate both the specificity of infringing material as well as a clear indication of the content's illicit nature.³⁸¹ While a bright-line rule such as this is valuable as a practical guidance for online services, an interpretation that renders a statutory element dormant is hardly an acceptable construction of the law.³⁸² Some scholars are concerned that such interpretation might encourage irresponsible practices by OSPs, who are more than willing to feign blindness despite an overwhelming evidence of third-party infringement.³⁸³

Nevertheless, it would be wrong to conclude, as many commentators have, that courts have entirely foreclosed the finding of red flags and, therefore, apparent knowledge.³⁸⁴ A different outcome can be reached when the inquiry shifts from the degree of piratical nature of the material to the degree of cynical character of conduct and intent on a service provider's part. This point will be further elaborated when we discuss the doctrine of willful blindness.³⁸⁵

which infringing activity is apparent"); *see also* *Hendrickson v. eBay Inc.*, 165 F. Supp. 2d 1082, 1092–93 (C.D. Cal. 2001) (holding that because plaintiff's written notifications do not comply substantially with § 512(c)(3)(A)(ii)'s adequate identification requirement, the Court does not consider those notices when evaluating the actual or constructive knowledge prong of the safe harbor test).

³⁸¹ *See supra* notes 290-295 and accompanying text.

³⁸² The copyright plaintiffs complained that courts repeatedly failed to devise a workable standard for apparent knowledge, while continued to reject virtually all types of evidence they had prepared to establish red-flag awareness. *See, e.g.*, Appellant's Brief at *50–52, *UMG Recording, Inc. v. Shelter Capital Partner LLC*, 2011 WL 6357788 (No. 09-56777) (9th Cir. Dec. 20, 2011).

³⁸³ *See, e.g.*, Ginsburg, *supra* note 64, at 598 (“[A]pparent’ does not mean ‘in fact illegal,’ nor does it mean ‘conclusively exists.’ Such an interpretation would allow the service provider to ‘turn a blind eye’ to infringements because the provider could claim that the possibility that some files might be fair use means that infringement can never be ‘apparent’ as to any file.”).

³⁸⁴ *See, e.g.*, Chang, *supra* note 31, at 219–21 (discussing the continuing legitimacy of the red flag test); *see also*, Amir Hassanabadi, *Viacom v. YouTube—All Eyes Blind: The Limits of the DMCA in a Web 2.0 World*, 26 *BERKELEY TECH. L.J.* 405, 435-436 (2011) (discussing the use of the red flag test by courts).

³⁸⁵ *See* S. REP. NO. 105-190, at 48 (1998) (referring to pirate directories); *see also* H.R. REP. NO 105-551(II), at 58 (1998) (discussing pirate directories); *see* Peter S. Menell, *Intellectual Property Issues: Assessing the DMCA Safe Harbors: The Good, the Bad, and the Ugly*, MEDIA INSTITUTE (Aug. 31, 2010), http://www.mediainstitute.org/new_site/IPI/2010/090110.php; *see infra* Part

iii. The Causes of Judicial Reluctance in Finding Red Flag Knowledge and the Legal Tension it Creates

There have been many explanations as to why courts have refused to adhere to the legislative intent in assessing the apparent knowledge requirement.³⁸⁶ Many commentators have emphasized the fact that the Congress simply underestimated the difficulty of ascertaining legality of copyrighted material on the Internet.³⁸⁷ This concern is demonstrated in *Viacom* where the plaintiff requested withdrawal of some 250 clips—which it had put into YouTube through its advertising agent as a “stealth marketing” scheme to create viral effects—from its complaint.³⁸⁸ This move, no doubt, caused a significant damage to Viacom’s claim and helped convince the court that ISPs should not be expected, as a matter of law, to figure out which content is legitimate.³⁸⁹

It is also possible that the courts’ avoidance of congressional guideline was due to their realization that the application of the red flag doctrine is outright contrary to the notice-centrality nature of the § 512(c)’s safe harbors.³⁹⁰ So far, courts seem settled to regard an OSP as a legitimate or responsible provider if it adequately implements the notice-and-takedown system and handles notices of claimed infringements with certain efficiency.³⁹¹ The straightforwardness of this approach is admittedly essential for the DMCA to preserve its independent knowledge standard and provide clear guidelines for online business.³⁹²

IV.C.2.3.

³⁸⁶ See Chang, *supra* note 31, at 215–19 (“[F]irst, to promote Internet development, free flow of information, and electronic commerce; second, to place the burden on the most efficient cost bearer; and third, to avoid higher costs to consumers”).

³⁸⁷ Eric Goldman, *UMG v. Shelter Capital: A Cautionary Tale of Rightsowner Overzealousness*, TECHNOLOGY & MARKETING LAW BLOG (Dec. 27, 2011, 8:19 AM), http://blog.ericgoldman.org/archives/2011/12/umg_v_shelter_c.htm; Hassanabadi, *supra* note 384, at 437–38.

³⁸⁸ Memorandum of Law in Support of Defendants’ Motion for Summary Judgment at 14–16, 40–41, *Viacom*, 718 F. Supp. 2d 514 (S.D.N.Y. 2010) (No. 07-2103) (discussing the clips at issue in the case).

³⁸⁹ *Viacom*, 718 F. Supp. 2d at 526–27.

³⁹⁰ See Hassanabadi, *supra* note 384, at 419 (discussing the insufficiency of general awareness in raising a red flag under the DMCA).

³⁹¹ *Id.* at 412–13.

³⁹² See H.R. REP. NO. 105-551, at 25 (1998) (distinguishing § 512(c)’s apparent knowledge standard from that of contributory infringement, in

However, courts' collective approach in dealing with red flag awareness also creates a significant tension in the balance of the DMCA.³⁹³ On one hand, it is true that the only way to guarantee the effectiveness of the DMCA, as a safe harbor, is through a close observance of the notice-and-takedown mechanism, and not a liberal application of the red flag test.³⁹⁴ On the other hand, it is an undeniable fact that the apparent knowledge standard is incorporated into § 512 as an alternative mechanism, in lieu of notice-based actual knowledge when the latter is not available.³⁹⁵

In this respect, to read the red flag test completely out of the statute would be to invite abuses from ill-intending online services.³⁹⁶ The case of an online music streaming service called Grooveshark can illustrate a fine example.³⁹⁷ Grooveshark gets the music by scanning users' computers and upload them to its servers.³⁹⁸ "It consider[ed] these files to be user generated content" and would not take them down unless it was supplied with a valid DMCA notice.³⁹⁹ Grooveshark cynically argued that its service is perfectly legal since it operates within the ambit of the DMCA safe harbors.⁴⁰⁰ In 2009, EMI was reported to enter into a music license agreement with Grooveshark—presumably because the music giant did not favor the option of spending resources fighting a DMCA lawsuit against a small, online music service.⁴⁰¹

As the Grooveshark case demonstrates, DMCA is primarily a

essence making clear that the differences are necessary to set the two standards apart).

³⁹³ See generally S. REP. NO. 105-190, at 66–68 (1998) (discussing changes to the DMCA to prevent misunderstandings by parties affected by it).

³⁹⁴ Hassanabadi, *supra* note 384, at 412–15.

³⁹⁵ S. REP. NO. 105-190, at 44–45 (discussing actual and apparent knowledge in the context of § 512 and the red flag test); H.R. REP. NO. 105-551, at 53–54 (referring to actual and apparent knowledge in the context of § 512 and the red flag test).

³⁹⁶ *Contra* Chang, *supra* note 31, at 203 (indicating that apparent knowledge has never been found under the red flag test); see S. REP. NO. 105-190, at 44, 49 (discussing the red flag test, and its applicability); H.R. REP. NO. 105-551, at 53 (1998).

³⁹⁷ See Menell, *supra* note 385.

³⁹⁸ *Id.*

³⁹⁹ *Id.*

⁴⁰⁰ *Id.*

⁴⁰¹ See Eliot Van Buskirk, *EMI Drops Suit Against Grooveshark Music Service, Licenses It Instead*, WIRED (Oct. 13, 2009, 12:00 PM), <http://www.wired.com/epicenter/2009/10/emi-drops-suit-against-grooveshark-music-service-licenses-it-instead/> (indicating that EMI licensed Grooveshark in an effort to avoid the costs of a lawsuit).

protective mechanism for online providers.⁴⁰² The “red flag” test, therefore, serves as a counter measure to screen out irresponsible and cynical online services. This is the balance that Congress struck with its enactment of the DMCA.⁴⁰³ It will not satisfy both sides of the conflict until courts can provide a more concrete and practical way of dealing with claims regarding apparent knowledge.⁴⁰⁴

Undoubtedly, the “apparent knowledge” and red flag test will continue to be litigated so long as its language appears in the text of § 512(c).⁴⁰⁵ Indeed, the courts’ failure to determine, with some practicality, when or how a red flag should be triggered has transformed DMCA disputes into ultra-expensive lawsuits.⁴⁰⁶ Plaintiffs who never sent a single valid DMCA notice, such as UMG, will continue to issue claims against DMCA-qualifying OSPs under various cognitive theories.⁴⁰⁷ Given that the legislative history of the DMCA is filled with doubtful language, the legal interpretation of “red flag” knowledge will continue to be a significant problem in the application of the § 512, causing both uncertainties and unintended consequences for online businesses.⁴⁰⁸

⁴⁰² See Menell, *supra* note 385.

⁴⁰³ See *generally id.*; see S. REP. NO. 105-190, at 49 (1998) (explaining Congressional rationale behind the “red flag” test and referencing the “balance”).

⁴⁰⁴ See *id.* (explaining the effect of the DMCA on OSP’s and content providers and how the legislation is problematic).

⁴⁰⁵ See *id.* (explaining how Congress’ attempt to balance the competing interests of content owners and OSP’s within § 512(c) is no longer adequate and instead provides leverage for OSP’s).

⁴⁰⁶ Google is reported to have paid over \$100 million in legal fees to defend itself against Viacom. Erick Schonfeld, *Google Spent \$100 Million Defending Against Viacom’s \$1 Billion Lawsuit*, TECHCRUNCH (July 15, 2010), <http://techcrunch.com/2010/07/15/google-viacom-100-million-lawsuit>.

⁴⁰⁷ See Chang, *supra* note 31, at 219 (explaining how the inadequacies of § 512(c) result in increased litigation and reduce the likelihood of cooperation between OSP’s and content owners).

⁴⁰⁸ For example, early legislative history classifies the § 512(c) as “a Good Samaritan defense” which implies that service providers who are to be protected by the safe harbor must strive to protect copyright in earnest. H.R. REP. NO. 105-551, at 25–26 (1998) (creating the appearance that the “apparent knowledge” standard leaves open a wide possibility that copyright holders may subject an OSP to liability by focusing on general intent of the OSP rather than going through troubles of providing information on infringing activity).

2. Red Flag Test and “Willful Blindness” Doctrine

As discussed in Part II, the willful blindness doctrine is a borrowed concept from criminal law and can be found in other areas of law, including secondary copyright liability.⁴⁰⁹ In the context of the apparent knowledge standard under the DMCA, willful blindness or the “blind eye” theory is explicitly discussed in the legislative report as an important indicator for establishing apparent knowledge in OSPs.⁴¹⁰ Because willful blindness is also an indicator of knowledge under contributory liability, Congress’ endorsement of the doctrine inevitably disturbs the hypothesis that the DMCA’s knowledge standard is not coextensive to that of secondary liability under common law.⁴¹¹ However, the Legislative Committee views the willful blindness doctrine as commensurable with the underlying principle of the DMCA, such that “[u]nder 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.”⁴¹²

a. Courts’ Receptiveness toward “Willful Blindness” Argument

Willful blindness is a remarkable doctrine because of the fact that courts are generally receptive to the argument that a defendant turned a blind eye to the red flag circumstance whereas other evidence failed to satisfy direct or apparent knowledge requirement.⁴¹³ The potency of willful blindness argument was demonstrated in *Columbia Picture Industries, Inc. v. Fung*, a secondary infringement dispute in online file-sharing context.⁴¹⁴ In *Fung*, Plaintiffs brought suit claiming that the defendant had infringed on their copyrights by hosting a P2P file-

⁴⁰⁹ *Global-Tech Appliances*, 131 S. Ct. 2060, 2068, 2071–72 (2011).

⁴¹⁰ S. REP. NO. 105-190, at 44, 48 (1998).

⁴¹¹ *See id.* at 43–44 (explaining that § 512(c) limits liability for service providers for claims of contributory infringement unless it can be shown that the service provider essentially ignored indicators of infringement).

⁴¹² *Id.* at 48.

⁴¹³ *See Viacom II*, 676 F.3d 19, 30–31, 34–35 (2d Cir. 2012) (holding that in appropriate circumstances a showing of “willful blindness” on the part of a service provider can satisfy the actual knowledge of specific infringement requirement under the DMCA).

⁴¹⁴ *Fung*, No 06-5578, 2009 WL 6355911, at *16–18 (C.D. Cal. Dec. 21, 2009) (explaining that defendants’ claim of being subjectively unaware of specific infringement amounts to willful blindness).

sharing network.⁴¹⁵ The defendant, Fung, raised an affirmative defense under § 512 (d) of the DMCA.⁴¹⁶ Interestingly, one of the defendant's arguments – relying on the Ninth Circuit's decision in *Subafilms, Ltd. v. MGM-Pathe Communications Co.* – is that the plaintiffs cannot bring a claim of secondary copyright infringement in a US court if the act of direct infringement occurred entirely outside the United States.⁴¹⁷

The *Fung* court overcame that limitation by holding that Fung was not qualified for the DMCA defense because it clearly had knowledge of infringement on account of its “willful ignorance of . . . apparent infringement”⁴¹⁸ According to *Fung* court:

Even under this stringent “willful ignorance” test, it is apparent that Defendants have “turned a blind eye to ‘red flags’ of obvious infringement.” Most importantly . . . even if [Defendant Fung's] downloads were done abroad and were not actionable under United States copyright law (and thus would not provide “actual knowledge” of illegal activity for purposes of 17 U.S.C. § 512(d)(1)(A)), Fung's actions show that Fung was aware that infringing material was available on the Defendant websites.⁴¹⁹

As this remarkable conclusion shows, the *Fung* court utilized the willful blindness doctrine to adduce evidence of overseas infringement and so established that the knowledge requirement had been fulfilled.⁴²⁰ The court reasoned that “[g]iven the ‘worldwide’ nature of the world-wide web, it would have been obvious that United States-based users could access these same infringing materials and thus engage in infringing acts.”⁴²¹

Similarly, in *Flava Works, Inc. v. Gunter*, the District Court of Northern District of Illinois held that the defendant Gunter had not qualified for protection under § 512(c) because it had not “adopted and reasonably implemented a ‘repeat infringer’ policy.”⁴²² The court based its conclusion on Gunter's failure to implement filters or identifiers to prevent repeated infringing

⁴¹⁵ *Id.* at *1.

⁴¹⁶ *Id.* at *15–16.

⁴¹⁷ *Id.* at *7–8 (citing *Subafilms, Ltd. v. MGM-Pathe Comm'ns Co.*, 24 F.3d 1088, 1098 (9th Cir.1994)).

⁴¹⁸ *Id.* at *16–17 (citing *UMG II*, 665 F. Supp. 2d 1099, 1108 (C.D. Cal. 2009)).

⁴¹⁹ *Id.* at *17.

⁴²⁰ *Fung*, 2009 WL 6355911, at *17.

⁴²¹ *Id.*

⁴²² *Flava Works*, 2011 WL 3205399, at *10 (N.D. Ill. July 27, 2011).

conduct as well as his failure to investigate and terminate actual recidivists.⁴²³

However, it was Gunter's attitude toward copyright enforcement that appalled the court and which led to his disqualification from the DMCA.⁴²⁴ According to the policy that Gunter adopted for the "myVidster" service, he would only remove the link to the content that his users uploaded if such content "would not otherwise be accessible by the public."⁴²⁵ Moreover, he advised copyright owners that the best way to deal with infringing content is by "contacting the websites that are hosting your content to help stop the future bookmarking of it on myVidster."⁴²⁶ The *Flava Works* court responded as follows: "This perspective is the epitome of 'willful blindness.' Gunter is not concerned about *copyright* infringement; he simply examines whether the material posted by the user is 'otherwise not [] accessible by the public[.]' . . . His definition of 'repeat infringer' does not encompass copyright law."⁴²⁷

The court then equated Gunter—based on his failure to take repeat infringement seriously—with a copyright thief such as Aimster, whose conduct was described by the Seventh Circuit as an "ostrich-like refusal to discover the extent to which its system was being used to infringe copyright. . . ."⁴²⁸

Cases such as *Fung* and *Flava Works* clearly testify that courts have tendency to heed evidence of apparent infringement when it is dressed up in the form of willful blindness.⁴²⁹ While it may be true that defendants such as Fung and Gunter are far-removed from being champions of copyrights, it is perplexing that their haughtily disdainful attitudes should be used as a factor in assessing their eligibility for DMCA protection.⁴³⁰ Nowhere in the

⁴²³ *Id.* at *8.

⁴²⁴ *See id.* (highlighting the defendant's remarks concerning his repeat infringer policy in order to demonstrate his attitude toward the activity concerned).

⁴²⁵ *Id.*

⁴²⁶ *Id.*

⁴²⁷ *Id.*

⁴²⁸ *Flava Works*, 2011 WL 3205399, at *10 (quoting *In re Aimster*, 334 F.3d 643, 655 (7th Cir. 2003)).

⁴²⁹ *See id.* at *7 (explaining the standard for willful blindness); *see Fung*, No. CV 06-5576 SVW(JCx), 2009 WL 6355911, at *16–18 (C.D. Cal. Dec. 21, 2009) (exemplifying evidence of apparent infringement).

⁴³⁰ *See Flava Works*, 2011 WL 3205399, at *10 (stating that Gunter's attitude is "'another piece of evidence' of contributory negligence"); *see Fung*, 2009 WL 6355911, at *5 (providing an example of a defendant with a disdainful attitude).

text of the DMCA, or in its legislative history, does it demand that a service provider must further the cause of copyright enforcement beyond adequate implementation of the notice-and-takedown system.⁴³¹

3. The Impact of Supreme Court's Formulation of Willful Blindness in Global Tech Appliances

The Supreme Court's recent rendition of the willful blindness doctrine in *Global-Tech Appliances* is likely to have implication on future interpretations of the doctrine in copyright context.⁴³² As previously discussed in Part II, the newly clarified notion of willful blindness shows that the test is a rather stringent one to meet.⁴³³ In the first place, the *Global-Tech* Court clearly stated that the standard of proof for willful blindness is close to that of actual knowledge.⁴³⁴ Thus, a mere objective indication that a defendant "should have known" of a substantial risk of wrongdoing would not satisfy willful blindness standard.⁴³⁵

Second, the finding of willful blindness also requires a determination of whether there is any "deliberate action" on part of a defendant to avoid learning of the fact.⁴³⁶ It is rather unclear as to what kind of "deliberate action" of shutting oneself from knowing would give rise to a willful blindness claim.⁴³⁷ What is clear, however, is that "willful blindness" is simply one species of a "but-for" test based on a proposition that a defendant *would have been* in possession of "a requisite knowledge," had he or she not taken a deliberate action to enclose herself from existing facts.⁴³⁸ Indeed, according to the Supreme Court, a willful blindness defendant is the one who "[was otherwise aware of] a high probability of wrongdoing and who can almost be said to

⁴³¹ See *University of California Guidelines for Compliance*, *supra* note 11 (defining prerequisites for limited liability, including "not hav[ing] actual notice . . . [and] upon notice . . . respond[ing] expeditiously to remove or disable the material").

⁴³² *Global-Tech Appliances*, 131 S. Ct. 2060, 2070–72 (2011).

⁴³³ See *supra* Part II.B.4.

⁴³⁴ See *Global-Tech Appliances*, 131 S. Ct. at 2071 (holding that willful blindness can be found "only where it can almost be said that the defendant actually knew").

⁴³⁵ *Id.* at 2070–71.

⁴³⁶ *Id.*

⁴³⁷ See *id.* at 2070 (stating that the Court of Appeals articulates the doctrine in different ways).

⁴³⁸ *Id.* at 2069–71.

have actually known the critical facts.”⁴³⁹

Because of its inherently stringent standard, the willful blindness test—at least in theory—should be met only where the requisite but-for causation is found.⁴⁴⁰ Nonetheless, the current applications of willful blindness in copyright disputes tend to disregard this but-for aspect of the test.⁴⁴¹ In fact, because an OSP has many options when designing its system of service, its choices of implementation or omission of certain features, can result in its losing the blessing of the DMCA.⁴⁴²

As we have seen, in *Flava Works*, the court placed an emphasis on the fact that Gunter failed to implement pre-publication filtering software for the myVidster service as an evidence of willful ignorance.⁴⁴³ This can be perceived as an identical outcome to the Seventh Circuit’s decision in *Aimster*, where the defendant P2P software distributor was found to be willfully blinding itself from ongoing infringement due to its deliberate action in implementing an encryption feature into its software.⁴⁴⁴

Likewise, in *Myxer Inc.*, the plaintiff Arista Records claimed that the defendant reluctance to implement Audible Magic fingerprinting system—the popular filtering software widely used among music-video-hosting OSPs—indicates the existence of willful blindness to widespread infringement.⁴⁴⁵ Arista argued that this willful blindness should lead to the finding of apparent knowledge under § 512(c)(1)(A)(ii), despite the fact that Myxer had a blameless record in handling copyright holders’ notices of claimed infringement.⁴⁴⁶ The court rejected plaintiff’s argument

⁴³⁹ *Id.* at 2070–71.

⁴⁴⁰ *Global-Tech Appliances*, 131 S. Ct. at 2070-71.

⁴⁴¹ *See id.* (showing how existing judicial analysis of willful blindness is limits the scope to exclude recklessness and negligence, which would therefore disregard but-for causation).

⁴⁴² *See, e.g., Flava Works*, 2011 WL 3205399, at *8 (N.D. Ill. July 27, 2011) (discussing the “fail[ure] to implement filters or identifiers to prevent repeat infringing conduct”).

⁴⁴³ *Id.* at *8.

⁴⁴⁴ *In re Aimster*, 334 F.3d 643, 650–51 (7th Cir. 2003).

⁴⁴⁵ *See Myxer Inc.*, 2011 U.S. Dist. LEXIS 109668 at *86–87 (C.D. Cal. Apr. 1, 2011). This issue also appeared in *UMG II*. In that case the plaintiff also argued that the defendant’s delay in implementing a preferred filtering system was an indication of its avoiding of apparent knowledge of infringement. *UMG II*, 665 F. Supp. 2d 1099, 1103 (C.D. Cal. 2009).

⁴⁴⁶ *Myxer Inc.*, 2011 U.S. Dist. LEXIS 109668 at *20–21, *23–26, *72, *76, *89 (showing that the records reflect Myxer did far more than DMCA requires it to do, even further investigating infringement pursuant to complaints and generally treated a complaint as a takedown notice).

by noting that the DMCA does not explicitly impose an obligation on a service provider to implement filtering technology and that “[t]aken alone, the failure to develop a filter would be insufficient to support liability.”⁴⁴⁷

Nonetheless, the *Myxer* court reserved a partial disclaimer in its opinion by noting that the use or non-use of filtering tools may be relevant to the finding of apparent knowledge.⁴⁴⁸ The court acknowledged that in its other decision, *Columbia Picture Industries v. Fung*, the court had found it “probative that defendants did not attempt to develop filtering tools or other means of diminishing the use of its product for infringement.”⁴⁴⁹ However, the *Myxer* court was willing to distinguish the more responsible defendant, Myxer, from the outrageous Fung for the purpose of finding willful blindness. According to the court, “[failure to implement filtering software] must be considered in context with other evidence to determine the existence of an unlawful objective on the part of the service provider.”⁴⁵⁰

As the aforementioned cases illustrate, “willful blindness” in online copyright litigation is a somewhat open question that can create uncertainty over the applications of the DMCA.⁴⁵¹ Nonetheless, the Supreme Court’s clarification of the doctrine in *Global Tech Appliances* suggests that the standard for determination of willful blindness should be a stringent one – where there is a clear causal link between the defendant’s ignorance and its deliberate action.⁴⁵² If courts in future copyright disputes take up the instruction, we might see a turnaround in the courts’ receptiveness towards willful blindness claims.⁴⁵³

a. Willful Blindness and “Copyright Thief” Discourse

One can notice, without much difficulty, that willful blindness claims often achieve their objective in establishing apparent or

⁴⁴⁷ *Id.* at *88 (citing *Fung*, No. CV 06-5576 SVW(JCx), 2009 WL 6355911, at *10 (C.D. Cal. Dec. 21, 2009)).

⁴⁴⁸ *Myxer Inc.*, 2011 U.S. Dist. LEXIS 109668 at *87.

⁴⁴⁹ *Id.* at *87–88 (quoting *Fung*, 2009 WL 6355911, at *11); *but cf.*, *UMG II*, 665 F. Supp. 2d at 1111–12 (holding that DMCA does not obligate a service provider to implement filtering system at all).

⁴⁵⁰ *Myxer Inc.*, 2011 U.S. Dist. LEXIS 109668 at *87–88.

⁴⁵¹ *See supra* Part IV.C.2.b.

⁴⁵² *See Global-Tech Appliances*, 131 S. Ct. 2060, 2070–71 (2011).

⁴⁵³ *See id.* at 2070–71 (speculating about the impact of the willful blindness scope limitation).

actual knowledge when plaintiffs could also prove that the defendant is a kind of copyright villain that the DMCA was not designed to protect.⁴⁵⁴ Painting a picture of a copyright defendant as a rogue enterprise can be a power tool in overcoming the stringent standard of willful blindness.⁴⁵⁵ However, while there might be some service providers that genuinely deserve such designation, plaintiffs' efforts to remove defendant OSPs from the DMCA—based on the existence of a red flag—could boil down to just name calling and shouting fire.⁴⁵⁶

One can find detailed elaborations of a defendant's atrocities against a plaintiff's copyright in most online copyright disputes.⁴⁵⁷ In *Fung*, for instance, the plaintiffs supported their claim that the defendants could not be eligible for DMCA safe harbor's protection on the basis that they were a part of infringing circles that illegally benefit from plaintiffs' proprietary content.⁴⁵⁸ In the conclusion of their willful blindness argument, the plaintiffs stated that “[i]n sum, defendants operate precisely the kinds of ‘obviously pirate’ sites that are denied safe harbor.”⁴⁵⁹

A similar kind of piratical discourse also played a central role in the plaintiff's argument in *Viacom International, Inc. v. YouTube*.⁴⁶⁰ In *Viacom*, the plaintiff tried to defeat YouTube's affirmative DMCA defense by focusing on YouTube's attitude and practice towards the use of copyrighted works in its early days of

⁴⁵⁴ See, e.g., *Myxer Inc.*, 2011 U.S. Dist. LEXIS 109668 at *92, *95–98, *107–109 (showing how the defendant is a potential example of a copyright villain).

⁴⁵⁵ See, e.g., *Fung*, No. CV 06-5576 SVW(JCx), 2009 WL 6355911, at *12, *19 (C.D. Cal. Dec. 21, 2009) (demonstrating the legal effectiveness of providing evidence of defendant's negative history of copyright infringement); Pablo Lluch, *FBI Kill Megaupload*, LA ECONOMÍA Y LA MADRE QUE LA. (Jan. 20, 2012, 3:21 AM), <http://pablolluch.blogspot.com/2012/01/fbi-kill-megaupload.html> (giving context for the term ‘copyright villain’).

⁴⁵⁶ See *Fung*, 2009 WL 6355911, at *12 (showing an example of the “name calling” and how—looking at the facts alone—painting an enterprise as “rogue” to fulfill a legal doctrine, may sometimes be an inequitable application of justice).

⁴⁵⁷ See *id.*; see cases cited *supra* note 445 (showing relatively similar grievances by plaintiffs in other cases).

⁴⁵⁸ See *id.* (pointing to the fact that the users on *Fung*'s websites were venerated for being copyright infringers).

⁴⁵⁹ Plaintiffs' Reply Memorandum of Points and Authorities in Support of Summary Judgment on Liability at 15, *Fung*, 2009 WL 6355911 (C.D. Cal. 2007) (No. 206CV05578).

⁴⁶⁰ See *Viacom*, 718 F. Supp. 2d 514, 522–23 (S.D.N.Y. 2010) (discussing Internet piracy, obvious infringement, and safe harbor status).

operation.⁴⁶¹ Viacom relied mostly on evidence from between 2005 and 2007 to support its contention “that YouTube was a ‘pirate site,’ a ‘rogue enabler of content theft’ and a ‘video Grokster’ whose ‘business model is completely sustained by pirated content.’”⁴⁶²

Viacom cited various kinds of evidence, including email correspondences between the founders of YouTube before it was sold to Google in 2008.⁴⁶³ Without a doubt, Viacom’s arguments and evidence based on YouTube’s “rogue practices” in the past contrasted sharply with YouTube’s arguments demonstrating what a legitimate business it has actually become in 2010.⁴⁶⁴ Some commentators have noted that Judge Stanton’s rejection of evidence of YouTube’s past mischief may raise a difficult issue of how courts should apply inducement liability based on OSP’s past practice.⁴⁶⁵ Perhaps, YouTube is a special case of a technology that morphs over time to the point that it finally erases any doubt as to its “substantial non-infringing uses.”⁴⁶⁶

Nonetheless the issue in Viacom is not about the application of *Sony’s* defense; it was primarily about DMCA eligibility of YouTube.⁴⁶⁷ In this regard, the strategy of the plaintiff in Viacom was unmistakable: Viacom was trying to convince the court that YouTube is, or at least used to be, a copyright miscreant, so that its claim regarding apparent knowledge and willful blindness could be favorably perceived by the court.⁴⁶⁸ As Viacom

⁴⁶¹ Memorandum of Law in Support of Viacom’s Motion for Partial Summary Judgment and Inapplicability of the Digital Millennium Copyright Act Safe Harbor Defense at 1; *Viacom*, 718 F. Supp. 2d 514.

⁴⁶² *See id.* at 2, 5–7.

⁴⁶³ For instance, Viacom contended that YouTube was willfully blinding itself of the infringing nature of its service, because its founders knew as of 2005 that “[y]ou can find truckloads of . . . copyrighted content . . . [if] you [are] actively searching for it.” *Id.* at 6–7.

⁴⁶⁴ *See* Memorandum of Law in Support of Defendants’ Motion for Summary Judgment, *supra* note 388, at 1–2 (expressing the legitimacy and impact of YouTube’s business since its inception).

⁴⁶⁵ *See, e.g.*, Eric Goldman, *Viacom v. YouTube Summary Judgment Motions Highlights*, TECH. & MARKETING LAW BLOG (Mar. 18, 2010, 4:08 PM), http://blog.ericgoldman.org/archives/2010/03/viacom_v_youtub.htm.

⁴⁶⁶ *See Napster II*, 239 F.3d 1004, 1020 (9th Cir. 2001) (demonstrating use of the term ‘substantial non-infringing use’).

⁴⁶⁷ *See Viacom II*, 676 F.3d 19, 29–30 (2d Cir. 2012) (referencing YouTube’s eligibility for the safe harbor provisions of the DMCA).

⁴⁶⁸ Memorandum of Law in Support of Viacom’s Motion for Partial Summary Judgment and Inapplicability of the Digital Millennium Copyright Act Safe Harbor Defense, *supra* note 461, at 1–2.

eloquently illustrated on how YouTube had proceeded in the face of widespread infringement: “[T]o say there were red flags everywhere on YouTube is a gross understatement. Defendants were not merely aware of red flags signaling rampant infringement; they rallied around them.”⁴⁶⁹ Viacom’s thesis thus concludes that the only way YouTube can escape copyright liability is through willful ignorance of the fact:

[Y]ouTube’s business plan intentionally rested on such infringement-driven traffic An entertainment business may not intentionally exploit copyrighted works to attract a large audience, but escape liability by closing its eyes to the specific infringing videos by which it implements that plan. Willful blindness does not negate Defendants’ culpability. It intensifies it.⁴⁷⁰

Ultimately, the *Viacom* court’s ruling in favor of YouTube may owe to the fact that YouTube has evolved from a “rogue” enterprise into a hugely successful and legitimate business.⁴⁷¹ By 2008, YouTube has matured into a legitimate player that everyone enjoys dealing with. Nonetheless, this evolution takes time and resources.⁴⁷² It would be impossible for YouTube of 2005 – which also means myriads of other start-up and small-sized OSPs – to survive copyright holders’ attacks on their attitudes and practices when dealing with user-committed infringement.⁴⁷³ To reinstate the central point of our discussion, “apparent” or “red flag” knowledge is not as dormant as many scholars have suggested.⁴⁷⁴ The doctrine of willful blindness is a potent ingredient for the purpose of establishing such knowledge.⁴⁷⁵ It has potential to sidestep the fundamental principle of the DMCA, which precludes imposing general duty of investigation –

⁴⁶⁹ *Id.* at 50.

⁴⁷⁰ *Id.* at 50–51.

⁴⁷¹ See Memorandum of Law in Support of Defendants’ Motion for Summary Judgment, *supra* note 388, at 1–3.

⁴⁷² See *id.* at 1–2.

⁴⁷³ See Mark A. Lemley, *Protect Innovators, Not Copyright Lawyers*, NAT’L LAW J. (Oct. 19, 2011), <http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202519418520&slreturn=1> (implying that early-stage Internet start-ups have limited financial resources to deal with copyright infringement).

⁴⁷⁴ See *infra* Part IV.C.1.b.

⁴⁷⁵ See *Fung*, No. CV 06-5576 SVW(JCx), 2009 WL 6355911, at *17–18 (C.D. Cal. Dec. 21, 2009) (determining that sufficient evidence existed to establish defendants’ awareness of red flags indicating defendants had to have engaged in willful blindness to avoid knowledge of their users’ infringement).

regarding specific and obvious infringement – on service providers.⁴⁷⁶ More importantly, willful blindness can be used to avoid difficulties in proving apparent knowledge based on evidence other than proper DMCA notices.⁴⁷⁷ Indeed, at least one court has held that “willful blindness” is probably the only viable mode of proving apparent knowledge.⁴⁷⁸

Because of courts’ reluctance to find “apparent knowledge” based on evidence other than valid DMCA notices, copyright plaintiffs are likely to shift their strategies toward establishing willful blindness via “copyright thief” discourse.⁴⁷⁹ The focus of dispute will therefore be shifted from the determination of knowledge to the inquiry of whether an OSP has a right kind of conscience toward copyright enforcement.⁴⁸⁰ However, it is also far from clear as to what kind of OSPs could be deemed a good and reasonable actor under the DMCA.⁴⁸¹

Unfortunately, as case law demonstrates, courts have tendency to be swayed by willful blindness discourse when a defendant does not show a serious attitude towards complaints of claimed infringement.⁴⁸² Thus, a service provider who relies on the lower threshold standard of the DMCA could still be susceptible to claims under the willful blindness doctrine.⁴⁸³

⁴⁷⁶ See Brief for Amicus Curiae Mp3tunes, Inc., in Support of Appellee’s at 12–13, *Viacom II*, 676 F.3d 19 (2d Cir. 2012) (No. 10-3342, 10-3270) (discussing the purpose of the DMCA in terms of ISP’s duty to investigate); see also *UMG II*, 665 F. Supp. 2d 1099, 1108 (C.D. Cal. 2009) (discussing investigative requirements or the lack thereof for service providers).

⁴⁷⁷ See *Fung*, 2009 WL 6355911, at *17–18 (discussing willful blindness in terms of knowledge).

⁴⁷⁸ *UMG II*, 665 F. Supp. 2d at 1108 (holding that “[i]n light of the principles articulated in *CCBill*... it takes willful ignorance of readily apparent infringement to find a ‘red flag.’”).

⁴⁷⁹ See *id.* at 1106 (assessing the defendant’s apparent knowledge based solely on evidence that constituted valid DMCA notices); see Plaintiffs’ Reply Memorandum of Points and Authorities in Support of Summary Judgment on Liability, *supra* note 459, at 14–15 (discussing “‘obviously pirate’” sites in terms of the safe harbor provision).

⁴⁸⁰ See *Capitol Records*, 821 F. Supp. 2d 627, 637–38 (S.D.N.Y. 2011) (discussing indicia of the defendant’s willful blindness).

⁴⁸¹ See *UMG II*, 665 F. Supp. 2d at 1110–11 (discussing whether defendant’s actions were taken in good faith).

⁴⁸² See, e.g., *Flava Works*, 2011 WL 3205399, at *8 (N.D. Ill. July 27, 2011) (holding that failure to implement filtering system and failure to investigate and respond to notices of infringement with respect to content and repeat infringers lead to finding of willful blindness); cf., *Myxer Inc.*, 2011 U.S. Dist. LEXIS 109668, at *88 (C.D. Cal. Apr. 1, 2011) (holding that failure to develop a filter alone would not lead to finding of apparent knowledge).

⁴⁸³ See *Flava Works*, 2011 WL 3205399, at *7–8 (finding that the defendant

Furthermore, since it is still subject to much debate as to what kind of deliberate action would be willfully blinding, at least in the Web 2.0 environment, willful blindness claims could significantly affect future application of the DMCA—regardless of how well an OSP is complying with the notice-and-takedown regime of § 512(c). These observations lead to an anticipation that future DMCA disputes will continue to be expensive, confusing, and detached from the DMCA's true goals.

b. The DMCA and Inducement Liability

As discussed in the Part II above, inducement copyright liability was introduced by the Supreme Court in *MGM Studios, Inc. v. Grokster*.⁴⁸⁴ There are two reasons that dissuade an argument that inducement liability claims can be relied on to disqualify an OSP from the DMCA's safe harbors.⁴⁸⁵ First, the DMCA was enacted in 1998, years before the Supreme Court in *Grokster* decided to import the inducement doctrine into copyright secondary liability jurisprudence.⁴⁸⁶ Second, the Court in *Grokster* only sought to address the problem of contributory liability in the online file-sharing context without any intention to discuss its impact on the DMCA.⁴⁸⁷

However, in *Fung*, the District Court of the Central District of California agreed with plaintiffs that a defendant whose conduct falls under copyright inducement liability can lose the benefits of the DMCA's safe harbor.⁴⁸⁸ Because Fung's conduct constituted "purposeful, culpable expression and conduct' aimed at promoting infringing uses of the website," the court held that Fung was not eligible for safe harbor's protection.⁴⁸⁹ Specifically, the court clarified its logic as follows:

[I]nducement liability and the Digital Millennium Copyright Act

was guilty of willful blindness toward the infringement that was occurring, due in part to the defendant's casual attitude toward the claims).

⁴⁸⁴ See NIMMER & NIMMER, *supra* note 46, at §12.04[A][5][a].

⁴⁸⁵ See *infra* notes 486–87 and accompanying text.

⁴⁸⁶ See Vicky Ku, *A Critique of the Digital Millennium Copyright Act's Exemption on Encryption Research: Is the Exemption Too Narrow?*, 7 YALE J. L. & TECH. 466, 474 (2005) (discussing the inception of the DMCA); see *Grokster I*, 545 U.S. 913, 929–30 (2005) (discussing inducement liability).

⁴⁸⁷ See *Grokster I*, 545 U.S. at 944 (discussing the question of what circumstances render an online file-sharing distributor liable for third-party use without any mention of the DMCA).

⁴⁸⁸ *Fung*, 2009 WL 6355911, at *18 (C.D. Cal. Dec. 21, 2009).

⁴⁸⁹ *Id.* at *15–16.

safe harbors are inherently contradictory. Inducement liability is based on active bad faith conduct aimed at promoting infringement; the statutory safe harbors are based on passive good faith conduct aimed at operating a legitimate internet business. Here, as discussed *supra*, Defendants are liable for inducement. There is no safe harbor for such conduct.⁴⁹⁰

In its assessment of inducement liability, the *Fung* court made much discussion of the willful blindness doctrine.⁴⁹¹ Thus, in concluding that the defendant was not entitled to the affirmative defense provided by the § 512(c) of the DMCA, the *Fung* court seemed to insinuate that eligibility for safe harbor's protection may not be limited only to the statutory requirements under the DMCA, but also contingent to inquiries regarding general malicious conduct of the defendant.⁴⁹²

V. THE NINTH CIRCUIT'S INTERPRETATION OF THE DMCA'S KNOWLEDGE STANDARD IN THE UMG-VEOH DISPUTE

On December 20, 2011, the Court of Appeal of the Ninth Circuit finally issued the much-anticipated decision that shed a significant light on how the knowledge as well as other requirements under § 512(c) should be interpreted and applied to online service providers that host third parties' copyrighted content.⁴⁹³ This decision, *UMG Recording, Inc. v. Shelter Capital Partner LLC*, is the Ninth Circuit's taking on complexities of the DMCA for the first time in four years, since the influential *Perfect 10 v. CCBill* decision.⁴⁹⁴

A. Overview

Veoh Networks (Veoh) is the operator of a video-hosting service that allows users to watch and share videos with other users online—much similar to YouTube. Apart from hosting content uploaded by users, Veoh also hosts authorized content made

⁴⁹⁰ *Id.* at *18.

⁴⁹¹ *See id.* at *16–18 (discussing whether the actions taken by defendant constituted willful blindness, and finding that they did).

⁴⁹² *See id.* at *18 (finding that the defendant was liable for inducement, which was based on active bad faith conduct, and therefore there was no safe harbor available).

⁴⁹³ *See UMG III*, 667 F.3d 1022, 1034–37 (9th Cir. 2011) (discussing the safe harbor provisions in § 512 of the DMCA).

⁴⁹⁴ *See id.* at 1038–39, 1042 (discussing the CCBill case with respect to § 512 of the DMCA); *CCBill*, 488 F.3d 1102, 1109 (9th Cir. 2007).

available by copyright holders (partner content).⁴⁹⁵ Since the official launch of the “Veoh” service in February 2007, Veoh Networks has been a frequent target of copyright lawsuits.⁴⁹⁶ These lawsuits revealed that although Veoh could not entirely prevent its users from engaging in copyright infringement, it is a service provider that made substantial efforts to comply with the requirements of § 512(c) of the DMCA.⁴⁹⁷

In *Io Group*, the first dispute in the Veoh saga, the District Court of Northern District of California found that Veoh took a number of steps to suppress user-committed copyright infringement – some of which even surpassed § 512(c)’s requirements.⁴⁹⁸ Rejecting the plaintiff’s theory that the DMCA imposes on a service provider the “entire burden of policing third-party copyrights on its website,” the court concluded that Veoh had done enough to be eligible for the statutory safe harbor.⁴⁹⁹ “[F]ar from encouraging copyright infringement,” the *Io Group* court opined, “Veoh has a strong DMCA policy, takes active steps to limit incidents of infringement on its website and works diligently to keep unauthorized works off its website.”⁵⁰⁰

While Veoh managed to prevail virtually over all instances of legal challenge, the cost of DMCA lawsuits proved too much for the company to sustain.⁵⁰¹ Veoh was reported to file for

⁴⁹⁵ *UMG II*, 665 F. Supp. 2d 1099, 1101 (C.D. Cal. 2009).

⁴⁹⁶ Dawn C. Chmielewski, *Veoh to Target YouTube Viewers*, L.A. TIMES (Feb. 13, 2007), <http://articles.latimes.com/print/2007/feb/13/business/fi-veoh13>; see Ingrid Lunden, *Video Portal Veoh Retains Equity Partners CRB to Explore Sale, Other Strategic Options*, TECHCRUNCH (Sept. 13, 2012), <http://techcrunch.com/2012/09/13/video-portal-veoh-retains-equity-partners-crb-to-explore-sale-other-strategic-options> (stating that Veoh was subjected to various copyright infringement lawsuits).

⁴⁹⁷ *UMG II*, 665 F. Supp. 2d at 1102–04 (discussing the efforts made by Veoh to preclude infringement on its site and comply with takedown requests). Records show that “when a copyright holder sends Veoh a notice of infringement that complies with the DMCA’s notice-and-takedown provisions, Veoh disables access to the allegedly infringing videos, often the same day that Veoh receives notice, or within a day or two of notice.” Moreover, “[s]ince April 2007, Veoh’s Senior Manager of Copyright Compliance has also investigated less formal complaints of infringement.” *Id.* at 1102–03.

⁴⁹⁸ See *Io Grp.*, 586 F. Supp. 2d 1132, 1137–38, 1145–46, 1150 (N.D. Cal. 2008) (discussing statutory requirements and the steps taken by Veoh). For example, Veoh adopted a sort of “fingerprint” filtering system where it did not only remove infringing content as per copyright holders’ requests but also prevented identical files from being uploaded back onto its system. *Id.* at 1138.

⁴⁹⁹ *Io Grp.*, 586 F. Supp. 2d at 1155.

⁵⁰⁰ *Id.*

⁵⁰¹ See Chloe Albanesius, *Veoh Co-Founder Confirms Bankruptcy*,

bankruptcy in February, 2010 and was subsequently acquired by Qlipso, an Israeli media-sharing company.⁵⁰² With Veoh going under, its investor, Shelter Capital Partners, became the only remaining defendant in the latest decision.⁵⁰³ The fact that a legitimate service provider such as Veoh had to go out of the business—despite its enterprise being perfectly legal—is a typically sad note in DMCA disputes.⁵⁰⁴ Nevertheless, our current DMCA jurisprudence owed much to Veoh’s ordeal. By the time the Veoh saga reached its final chapter, the knowledge standard and other threshold requirements under the DMCA has become significantly more lucid than when the first legal complaint was filed against Veoh in 2006.⁵⁰⁵

B. Background of the UMG-Veoh Dispute

In September 2007 UMG instigated its lawsuit against Veoh for both direct and secondary infringement liability including inducement liability.⁵⁰⁶ Universal Music Group (UMG) controls the rights to many copyrighted sound recordings and musical compositions as it is one of the largest recording and music publishing companies.⁵⁰⁷ It is undisputed that many of UMG’s

PCMAG.COM (Feb. 12, 2010, 9:36 AM), <http://www.pcmag.com/article2/0,2817,2359105,00.asp> (stating that despite its victories in litigation, Veoh filed for bankruptcy due in part to the cost of defending multiple lawsuits).

⁵⁰² Don Reisinger, *Qlipso Acquires Video Site Veoh’s Assets*, CNET.COM (Apr. 7, 2010, 3:13 PM), http://news.cnet.com/8301-13506_3-20001960-17.

⁵⁰³ See *UMG III*, 667 F.3d 1022, 1029 n.3 (9th Cir. 2011) (showing that Shelter Capital was an investor of co-defendant Veoh in the “latest” case brought to trial).

⁵⁰⁴ Albanesius, *supra* note 501. After the company filed for bankruptcy, Dmitry Shapiro, the co-founder of Veoh Networks, remarked: “[w]hile we made every effort to convince them that we were not their enemy and had not infringed on their content, they pursued a relentless war of attrition against us in federal court.” *Id.*

⁵⁰⁵ Terry Banes, *UMG Loses Appeal Against Video-Sharing Site*, THOMSON REUTERS NEWS & INSIGHT (Dec. 20, 2011), http://newsandinsight.thomsonreuters.com/Legal/News/2011/12_-_December/UMG_loses_appeal_against_video-sharing_site/.

⁵⁰⁶ See *UMG Recordings, Inc. v. Veoh Networks, Inc. (UMG I)*, 620 F. Supp. 2d 1081, 1082 (C.D. Cal. 2008) (stating that UMG sued “Veoh and Veoh’s investors for direct, contributory, and vicarious copyright infringement, and for inducement of copyright infringement”).

⁵⁰⁷ See *Overview*, UNIVERSAL MUSIC GRP, <http://www.universalmusic.com/company> (last visited Nov. 3, 2012) (providing an overview of Universal Music Group’s history and operations of Universal Music Group’s numerous copyrighted works).

copyrighted videos and recorded music were uploaded onto the Veoh service without authorization, because UMG and Veoh were not content partners.⁵⁰⁸ Nonetheless, UMG itself never supplied any DMCA complying notice to inform Veoh about claimed direct infringements until its motion was filed.⁵⁰⁹ UMG's decision to forego the DMCA notices was due to its "belie[f] that it [was] not obligated under the DMCA 'to identify each instance in which Veoh is displaying unauthorized content.'"⁵¹⁰ Prior to UMG filing its complaint in September 2007, the "only notices Veoh received regarding alleged infringements of UMG's works were sent by the Recording Industry Association of America," but they were acting as UMG's agent.⁵¹¹

Since UMG never sent Veoh any notice of claimed infringement, UMG did not base its claim on the ground that Veoh's implementation of notice-and-takedown procedure has anything left to be desired.⁵¹² Rather, the plaintiff, relying on various statutory interpretations, moved for partial summary judgment on the basis that Veoh is not entitled to an affirmative defense under § 512(c) at all.⁵¹³

Specifically, UMG claimed that Veoh's automatic operations that result in modification of uploaded files – in order to make it easier for other users to locate the video for subsequent access and viewing – necessarily disqualify Veoh from § 512(c)'s safe harbor because they do not constitute operations "by reason of storage at the direction of users."⁵¹⁴ In other words, UMG endorsed an interpretation that § 512(c) applies only to operational features that provide or constitute storage – and nothing more.⁵¹⁵

The District Court, however, declined to accept UMG's narrow interpretation of the statute. The *UMG I* court held that the clear

⁵⁰⁸ *UMG I*, 620 F. Supp. 2d at 1085.

⁵⁰⁹ *Id.*

⁵¹⁰ *Id.*

⁵¹¹ *UMG II*, 665 F. Supp. 2d at 1104.

⁵¹² *Id.* at 1108.

⁵¹³ *UMG I*, 620 F. Supp. 2d at 1082.

⁵¹⁴ *Id.* at 1083–84. The four contested operations include: "(1) automatically creating 'Flash-formatted' copies of video files uploaded by users; (2) automatically creating copies of uploaded video files that are comprised of smaller 'chunks' of the original file; (3) allowing users to access uploaded videos via a technology called 'streaming'; (4) allowing users to access uploaded videos by downloading whole video files." *Id.* at 1083.

⁵¹⁵ See *UMG I*, 620 F. Supp. 2d at 1083, 1092 (holding that Veoh's operational Internet-based service falls within the scope of § 512(c)).

language of the DMCA signifies congressional intent to extend protection to “functions other than mere storage; it applies to ‘infringement of copyright by reason of the storage at the direction of a user’”⁵¹⁶

Following the District Court’s ruling in *UMG I*, Veoh moved for summary judgment that it had satisfied the remaining requirements of § 512(c).⁵¹⁷ Even though UMG never informed Veoh of specific instances of infringement by proper DMCA notices, it continued to argue that Veoh had both actual knowledge as well as the apparent knowledge of infringing content residing on its site. UMG’s cognitive theory is largely based on its belief that the DMCA does not limit the finding of either actual or apparent knowledge to just written information that complies with the notification requirement under § 512(c)(3).⁵¹⁸

First, UMG contended that Veoh’s actual knowledge of infringement was evident from several pieces of information, including Veoh’s engagement in hosting and displaying musical content, and the fact that ads’ words which Veoh purchased from search engines included names of music videos under UMG’s control.⁵¹⁹ Not persuaded, the court brushed aside UMG’s audacious argument that general awareness of certain types of content could, alone, translate into actual knowledge.⁵²⁰ The flaw in UMG’s argument, the court remarked, was that the DMCA would not allow a finding of actual knowledge with anything less than knowledge of specific infringement.⁵²¹

Second, the *UMG II* court rejected the plaintiff’s argument that non-DMCA-compliant notices—supplied by RIAA and which identified artists’ names—should obligate ISP to further search for infringing material because they do not impart information “*reasonably sufficient* to permit the service provider to locate the

⁵¹⁶ *Id.* at 1089.

⁵¹⁷ *UMG II*, 665 F. Supp. 2d at 1101.

⁵¹⁸ *See id.* at 1106, 1110 (supporting UMG’s argument about § 512(c)(3) by pointing to how the RIAA seemed to fulfill that provision by providing a representative list of names and works that were infringed).

⁵¹⁹ *Id.* at 1108–09.

⁵²⁰ *Id.* at 1109–10.

⁵²¹ *Id.* at 1108–09 (“UMG’s theory would also make the DMCA’s notice-and-takedown provisions completely superfluous because any service provider that hosted copyrighted material would be disqualified from the section 512(c) safe harbor regardless of whether the copyright holder gave notice or whether the service provider otherwise acquired actual or constructive knowledge of specific infringements.”).

material” as required by § 512(c)(3)(A)(iii).⁵²²

As for apparent knowledge of infringing facts and circumstances, UMG began by arguing that such knowledge cannot be disputed based on factual evidence that Veoh’s founders, employees, and investors are all aware of the widespread infringement that was transpiring on Veoh’s system.⁵²³ The court dismissed UMG’s evidence as a similar attempt to establish culpable knowledge based on mere general awareness of infringement. This argument, the court reasoned, belies the congressional intent that seeks to shield service providers from myriad of instances of copyright liability, upon which these providers may trip in ordinary course of their operations.⁵²⁴

The most interesting point of the *UMG II* court’s analysis of apparent knowledge is the court’s suggestion that the only way to establish red flag awareness is perhaps through evidence of “willful ignorance.”⁵²⁵ The court did not explicitly reveal the source from which it derived such conclusion.⁵²⁶ However, it is highly probable that the court took the hint from the language of the legislative history:

[A] service provider need not monitor its service or affirmatively seek facts indicating infringing activity . . . in order to claim this limitation on liability. However, if the service provider becomes aware of a ‘red flag’ from which infringing activity is apparent, it will lose the limitation of liability if it takes no action.⁵²⁷

UMG then rallied another argument, claiming that Veoh’s delay in implementing Audible Magic, an audio fingerprinting filtering system, demonstrated Veoh’s intention to avoid gaining knowledge by tugging its head in the sand.⁵²⁸ The court, however, appeared unmoved by UMG’s rhetoric. Veoh’s unblemished record in administering the DMCA takedown policy and the efforts it put into preventing infringement made this argument

⁵²² *Id.* at 1110.

⁵²³ *UMG II*, 665 F. Supp. 2d at 1111.

⁵²⁴ *Id.*

⁵²⁵ *Id.* at 1108 (holding that “it takes willful ignorance of readily apparent infringement to find a ‘red flag’”).

⁵²⁶ *See id.* (noting that the court investigates “facts and circumstances” to determine what constitutes infringement, but does not rely on any other authority for willful ignorance to fulfill the red flag test).

⁵²⁷ *Id.*

⁵²⁸ *Id.* at 1111.

sound hollow.⁵²⁹ Moreover, the court noted that the DMCA does not obligate a service provider to implement filtering technology at all.⁵³⁰

Next, the *UMG II* court turned to address the issue whether Veoh is to be excluded from the § 512(c)'s safe harbor on account of its "right and ability" to control the infringement.⁵³¹ According to UMG, the general ability to control operation of the system and the ability to take down content is enough to render an OSP unfit for the statutory protection – especially for a service provider like Veoh who has an ability to search for and identify potentially infringing material.⁵³² The *UMG II* court disagreed, deeming such conclusion to be contrary to the DMCA's objective, since virtually all service providers would then be disqualified.⁵³³ The court also distinguished the precedents relied on by UMG— all of which construed the control element in the context of judicially created doctrine of vicarious infringement – and the case at hand.⁵³⁴ Nonetheless, the court did not go far enough as to reach the conclusion that the control element under the DMCA must be construed independently from the common law vicarious liability doctrine.⁵³⁵

C. *The Ninth Circuit's UMG III Decision*

UMG appealed the District Court's decisions in *UMG I & II* to the Court of Appeals of the Ninth Circuit. On December 20, 2011, Judge Fisher, in an opinion written for the Ninth Circuit, affirmed the District Court's determination on summary judgment that Veoh was entitled to § 512(c)'s safe-harbor protection.⁵³⁶ The *UMG III* court reorganized UMG's argument into three major issues, namely 1) whether Veoh's tampering with users' uploaded files disqualifies it from the protection under § 512(c)(1) which protects a service provider for "infringement of copyright by reason of the storage at the direction of a user . . ."; 2) whether Veoh had the requisite level of knowledge under § 512(c)(1)(A); and 3) whether Veoh had "right

⁵²⁹ *UMG II*, 665 F. Supp. 2d at 1111–12.

⁵³⁰ *Id.*

⁵³¹ *Id.* at 1112.

⁵³² *Id.* at 1113–14.

⁵³³ *Id.*

⁵³⁴ *Id.* at 1114–15.

⁵³⁵ *UMG II*, 665 F. Supp. 2d at 1115–16.

⁵³⁶ *UMG III*, 667 F.3d at 1026 (9th Cir. 2011).

and ability to control,” under § 512(c)(1)(B), with regard to infringing activities from which it received a direct financial benefit.⁵³⁷

In the following sections, our discussion shall be confined to issues closely pertaining to our foregoing analysis of the DMCA’s knowledge standard, which is the focus of this paper.⁵³⁸

1. UMG’s Arguments

The central tenet of UMG’s criticism of the District Court’s decision granting summary judgment in favor of Veoh is grounded upon its disagreement that different rules should be applied for determining secondary liability “in the internet realm.”⁵³⁹ From UMG’s perspective, there can be no serious doubt as to whether Veoh’s business encouraged or even participated in illegal uses of copyrighted content, as “[h]istorically, businesses like Veoh that engaged in the unauthorized distribution of copyrighted content were considered pirates and dealt with accordingly—they were found liable for damages and enjoined.”⁵⁴⁰

In its appellate brief, UMG continued to advance its various interpretations of the text of the DMCA by making constant allusions as to how those terms have been interpreted in secondary liability context.⁵⁴¹

a. UMG’s Argument on Actual Knowledge

UMG anchored its argument regarding the actual knowledge standard of the DMCA on the theory that “actual knowledge” is a finding based on a service provider’s “own awareness of infringing activity on its servers,” rather than a consideration based on types of evidence.⁵⁴² Pursuant to this logic, UMG claimed that the District Court erred in applying the DMCA when it focused on “characteriz[ing] certain evidence presented by UMG as insufficient as a matter of law,” instead of trying to identify a standard for finding of actual knowledge.⁵⁴³

UMG, however, never explained as to why it had foregone the

⁵³⁷ *Id.* at 1030–31.

⁵³⁸ *See supra* Part I.

⁵³⁹ UMG’s Opening Brief, *supra* note 20, at 4.

⁵⁴⁰ *Id.*

⁵⁴¹ *See id.* at 34, 36–37, 39, 41–42, 44–45, 49, 67–68 (alluding to various interpretations of how the DMCA relates to secondary liability).

⁵⁴² *Id.* at 49–51.

⁵⁴³ *Id.* at 49.

DMCA notice in the first place. Instead, the giant record company attempted to circumvent the notice-centrality aspect of the DMCA's actual knowledge requirement by utilizing two modes of argument.⁵⁴⁴

First, UMG sidestepped the notice-centrality principle by arguing that specific knowledge from a compliant notice is not apposite when the operator of an Internet site is “displaying and distributing infringing material on its *own system*.”⁵⁴⁵ According to UMG, if a service provider displays or distributes copyrighted works on its own system, then the *CCBill* court's famous statement— “[t]he DMCA notification procedures place the [entire] burden of policing copyright infringement . . . [on the copyright owner]” —cannot be conclusively relied on to dismiss a claim of actual knowledge.⁵⁴⁶ Consequently, given “evidence of Veoh's acknowledgement that it knew it was hosting on its [own site] thousands of [copyrighted video files],” UMG contended that actual knowledge should be found.⁵⁴⁷

Second, UMG tacitly argued that the “actual knowledge” requirement under § 512(c)(1)(A)(i) is the same standard as the requisite knowledge under contributory infringement doctrine.⁵⁴⁸ Under this standard, UMG explained, a service provider would be in possession of actual knowledge if it knew that certain category of copyrighted content, such as music, is being hosted or shared through its system.⁵⁴⁹ More specifically, UMG asserted that when a service provider can identify and assign category of content to files that it is hosting—which Veoh apparently did by “tag[ging]” thousands of video files as “music video[s]”—it possesses not merely general awareness of copyrighted content but actual knowledge of unauthorized infringements.⁵⁵⁰

This aspect of UMG's theory is apparently based on the Ninth Circuit's decision in *Napster*, which held that a statement by a Napster co-founder—“acknowledging that users were [swapping] copyrighted music”—was evidence of actual knowledge.⁵⁵¹ Indeed,

⁵⁴⁴ See *id.* at 49–56 (discussing the District Court's improper construction of the knowledge requirement and the consequences of its ruling).

⁵⁴⁵ UMG's Opening Brief, *supra* note 20, at 51, n.12.

⁵⁴⁶ *Id.* at 50–51.

⁵⁴⁷ *Id.* at 49–50.

⁵⁴⁸ *Id.* at 51–52.

⁵⁴⁹ UMG's Opening Brief, *supra* note 20, at 52–53.

⁵⁵⁰ *Id.* at 56–59.

⁵⁵¹ *Id.* at 50. UMG also introduced similar evidence that Veoh Networks did the same thing when it gave an analysis of its own site, through which it

UMG argued that a separate District Court in the Central District which decided *Fung* adopted this approach when it held that “awareness that infringing material was available on the [D]efendant’s website[s] was sufficient to support finding of knowledge under the DMCA.”⁵⁵²

In this regard, UMG objected to the District Court’s observation that “actual knowledge” under the DMCA should be interpreted differently from case law addressing contributory liability.⁵⁵³ In UMG’s eyes, the District Court’s rejecting to apply *Napster*’s knowledge standard constituted a deviance from the Ninth Circuit’s precedent.⁵⁵⁴

b. UMG’s Argument on Apparent Knowledge

With regard to “apparent” or “red flag” knowledge, UMG argued that the District Court’s interpretation of § 512(c)(1)(A)(ii) was very narrow.⁵⁵⁵ UMG was in firm belief that the inclusion of subsection (A)(ii) was meant to create a separate standard different from actual knowledge in subsection (A)(i).⁵⁵⁶ According to UMG, the language and structure of § 512(c)(1)(A) clearly suggested that Congress intended to establish a standard of “something less than actual knowledge of infringement [to] trigger[] an obligation to remove material or face monetary liability.”⁵⁵⁷

UMG also raised doubt as to whether the finding of red flag is at all possible, if apparent “facts and circumstances” cannot require a service provider to make any further investigation.⁵⁵⁸ To support its argument UMG pointed to legislative history—albeit an older version of a House Report—asserting that Congress in fact approves the proposition that a service provider “may have an obligation to check further,” once it becomes aware of facts and information pertaining to infringement.⁵⁵⁹

determined that “[Veoh’s] number one category of searched and viewed content [was] Music.” *Id.* at 18–20.

⁵⁵² *Id.* at 52.

⁵⁵³ *Id.* at 49–51.

⁵⁵⁴ *Id.* at 50–51.

⁵⁵⁵ UMG’s Opening Brief, *supra* note 20, at 53 (arguing that the District Court’s standard for when a service provider is required to take down infringing material is inconsistent with the Congressional intent of the DMCA).

⁵⁵⁶ *Id.*

⁵⁵⁷ *Id.*

⁵⁵⁸ *Id.*

⁵⁵⁹ *Id.*

In its discussion of red flag knowledge, UMG noticeably made no reference whatsoever to a more current version of legislative reports.⁵⁶⁰ At first blush, this seemed to be a curious move. However, UMG's purpose in refraining from engaging in a legislative history discussion was reflected in its underlying strategy to focus its arguments on the plain meaning and structure of the statutory text—rather than on what it referred to as “broad [and] precatory language” of the statute's legislative records.⁵⁶¹

UMG's disapproval of the District Court's reliance on legislative history for the interpretation of the “red flag” test also underscored its objection against the *UMG II* court's holding that a “red flag” can only be found when there is evidence of “willful ignorance.”⁵⁶² UMG claimed that such conclusion is groundless and not supported by any authority.⁵⁶³ Obvious enough, UMG staunchly believed that Congress had envisioned “apparent knowledge” standard under § 512(c) to be met in a simpler way. In this regard, UMG was apparently aware that the standard of willful blindness is closer to that of actual knowledge—and that it would have little chance in proving apparent knowledge under such theory.⁵⁶⁴ Veoh's strong performance in administering its takedown system and UMG's limited evidence on Veoh's willful blindness seem to negate that possibility.⁵⁶⁵

c. UMG's Argument on Willful Blindness

Despite its reluctance to admit that willful blindness is the only way to meet the requirement of apparent knowledge, UMG

⁵⁶⁰ See UMG's Opening Brief, *supra* note 20, at 38, 43, 53, 67, 75 (showing that repeated citations were made to an outdated House Report from the 105th Congress, which convened in the year 1998); see also H.R. REP. NO. 105-551, pt.1, at 1 (1998).

⁵⁶¹ UMG's Opening Brief, *supra* note 20, at 53.

⁵⁶² *Id.* at 53, 64. On the contrary, this point of ruling is vigorously supported by Veoh: “Apparent knowledge for purposes of [s]ection 512(c)(1)(A)(ii) requires evidence that a service provider turned a ‘blind eye’ to red flags of obvious infringement.” Brief of Appellee Veoh Networks, Inc. at 40, *UMG III*, 667 F.3d 1022 (9th Cir. 2011) [hereinafter Veoh's Opening Brief].

⁵⁶³ UMG's Opening Brief, *supra* note 20, at 52.

⁵⁶⁴ See *id.* at 53 (explaining that Congress intended for apparent knowledge to be a less stringent standard than actual knowledge, such that infringement could more readily proven than the standard presented by the District Court).

⁵⁶⁵ See Veoh's Opening Brief, *supra* note 562, at 11–17, 21–22, 26, 34, 42–44 (explaining the immense functionality of Veoh's infringement removal systems and the nominal amount of evidence provided by UMG).

maintained that it had produced ample evidence demonstrating Veoh's willful blindness.⁵⁶⁶ For UMG, the willful blindness doctrine is not, as the *UMG II* court had suggested, just a method of proving apparent knowledge.⁵⁶⁷ Instead, UMG argued that willful blindness is a general test in finding knowledge, which can be applied to establish either actual knowledge or apparent knowledge.⁵⁶⁸ UMG relied on the Seventh Circuit's application of the doctrine in *Aimster* as the main authority in support of its argument.⁵⁶⁹

UMG recommended that the court apply the willful blindness doctrine in this DMCA dispute.⁵⁷⁰ UMG did not challenge the notion that there should be distinctions between different sources of knowledge under the DMCA.⁵⁷¹ It argued, nonetheless, that a service provider must sometimes undertake an investigation to locate and disable infringing material on its system.⁵⁷² After all, according to UMG, the true purpose of willful blindness doctrine is to "prevent[] a service provider from willfully ignoring other sources of knowledge that do not comply with the notice and takedown requirements."⁵⁷³

UMG relied on many pieces of evidence in supporting its claim that Veoh willfully ignored facts and circumstances of infringement.⁵⁷⁴ Most of these claims, however, do not indicate willful ignorance because they merely emphasize the fact that Veoh should have been aware of some patterns of infringing circumstances.⁵⁷⁵ UMG's evidence largely failed to illustrate any

⁵⁶⁶ UMG's Opening Brief, *supra* note 20, at 63–64 (indicating that although UMG disagrees as to the standard applied, it believes that it has adequately demonstrated willful blindness based on the conduct of Veoh).

⁵⁶⁷ *See id.* at 50–53 (suggesting that the District Court incorrectly applied a test in which willful blindness is a response to actual notice and is thus simultaneously actual *and* apparent infringement).

⁵⁶⁸ *See id.* at 52–53 (discussing Congressional intent that justifies the belief that willful blindness can lead to either actual or apparent knowledge).

⁵⁶⁹ *Id.* at 52. UMG quoted a passage from the *In re Aimster* opinion that "[w]illful blindness is knowledge in copyright law . . . as it is in the law generally." *Id.*

⁵⁷⁰ Reply Brief of Appellants at 34–35, *UMG III*, 667 F.3d 1022 (9th Cir. 2011) (No. 09-56777) [hereinafter UMG's Reply Brief] (presenting UMG's forthright interpretation of *Aimster* and § 512(c)(1)(A) of the DMCA).

⁵⁷¹ *Id.* at 24–25 (showing how UMG believed the distinctions in knowledge were "sensible").

⁵⁷² UMG's Opening Brief, *supra* note 20, at 53.

⁵⁷³ UMG's Reply Brief, *supra* note 570, at 24.

⁵⁷⁴ UMG's Opening Brief, *supra* note 20, at 20–22, 57, 61–62.

⁵⁷⁵ *See* Veoh's Opening Brief, *supra* note 562, at 35, 37–38, 41–44 (indicating

probative action Veoh deliberately took to avoid encountering with these known facts.⁵⁷⁶ UMG, however, continued to root its claims of willful blindness on the its strongest argument that Veoh's deliberate postponement in implementing certain digital filtering technology, known as "Audible Magic," demonstrated the OSP's intent to avoid the discovery of copyrighted material.⁵⁷⁷ UMG claimed that earlier implementation of such technology would have allowed Veoh to discover and disable "the unauthorized display and distribution of thousands of infringing videos."⁵⁷⁸

2. The Ninth Circuit's Decision

The Ninth Circuit's analysis of the DMCA is largely in accord with this paper's hypothesis that the drafters of the DMCA intended the safe harbor's key elements to be determined by different standards from those under the common law secondary liability doctrine.⁵⁷⁹ The court rejected UMG's fundamental premise that § 512(c) of the DMCA should be narrowly interpreted.⁵⁸⁰ The court also refused to restrict its interpretative focus just to the text of the DMCA.⁵⁸¹ Instead, the court adopted an integrated approach of combining interpretation of the statutory text's plain meanings with suggestions and insights from the "language, structure, purpose, and legislative history" of the DMCA.⁵⁸²

that as UMG did not provide Veoh with any actual notice, the only potential awareness that Veoh may have had was an overly generalized one). For example, UMG claimed that Veoh had developed sophisticated searching tools that could suggest other related videos, including other infringing videos when a user searched for a copyrighted music video. Veoh's tools. Thus, "Veoh chose . . . to ignore all of this information and all of these tools in order to avoid finding evidence of infringement on its service." UMG's Opening Brief, *supra* note 20, at 61–62.

⁵⁷⁶ *UMG III*, 667 F.3d 1022, 1036, 1043 (9th Cir. 2011).

⁵⁷⁷ *See* UMG's Opening Brief, *supra* note 20, at 63–64 (discussing "Audible Magic" as one possible tool that allowed Veoh to access technology that could enable it to remove infringing material, but instead elected to wait).

⁵⁷⁸ *See id.* at 21, 64 (according to UMG, immediately after the filter was finally implemented, Veoh discovered and removed more than 60,000 unauthorized videos).

⁵⁷⁹ *See UMG III*, 667 F.3d 1022, 1042–44 (discussing the differences in safe harbor provisions and common law liability).

⁵⁸⁰ *Id.* at 1031, 1034–37.

⁵⁸¹ *See id.* at 1031, 1044 (discussing the legislative intent of Congress in enacting and putting certain provisions in the DMCA).

⁵⁸² *Id.* at 1044–45.

a. Rejecting UMG's "general awareness" theory

The Ninth Circuit rejected UMG's categorical assumption that if an OSP hosts certain type of content—notably music—it must have a general knowledge that its service is being used for infringement. The court held that:

[M]erely hosting a category of copyrightable content, such as music videos, with the general knowledge that one's services could be used to share infringing material, is insufficient to meet the actual knowledge requirement under § 512(c)(1)(A)(i).⁵⁸³

The *UMG III* court disagreed with UMG's contention that the District Court erred by limiting circumstances in which a provider may be found to possess actual knowledge under § 512(c)(1)(A)(i).⁵⁸⁴ The court's holding clearly demonstrates its endorsement of the principle that § 512(c) of the DMCA is essentially a notice centrality regime before anything else.⁵⁸⁵ Thus, UMG's own failure to adhere to the DMCA's notice protocol "stripped it of the most powerful evidence of a service provider's knowledge—actual notice of infringement from the copyright holder."⁵⁸⁶ To hold otherwise, the court opined, would be to render the § 512(c) a "dead letter" instead of an active safe harbor.⁵⁸⁷

Interestingly, in addressing UMG's reliance on the Ninth Circuit's decision in *Napster*, the court remarked that the general knowledge theory is also not supported in contributory liability case law.⁵⁸⁸ Specifically, the *UMG III* court brushed aside as misplaced UMG's contention that actual knowledge of infringement should be found when the operator of an Internet site displays and distributes infringing material on its own system.⁵⁸⁹ These arguments, the court believed, belied the doctrine articulated by the Supreme Court in *Sony*.⁵⁹⁰ Contrary to

⁵⁸³ *Id.* at 1037–38.

⁵⁸⁴ *See id.* at 1036 (discussing the District Court's decision, in which the Court of Appeals ultimately sided with rather than UMG regarding actual knowledge circumstances).

⁵⁸⁵ *See UMG III*, 667 F.3d at 1039–40 (discussing notice requirements in terms of § 512(c) of the DMCA).

⁵⁸⁶ *Id.* at 1036 (quoting *Corbis Corp.*, 351 F. Supp. 2d 1090, 1107 (W.D. Wash. 2004)).

⁵⁸⁷ *UMG III*, 667 F.3d at 1037–38.

⁵⁸⁸ *See id.* at 1037–38 (discussing general knowledge and how it is not a supported approach).

⁵⁸⁹ *See id.* (discussing why UMG's interpretation was faulty).

⁵⁹⁰ *Id.* (citing *Sony*, 464 U.S. 417, 439, 442 (1984), *superseded by statute*,

UMG's argument, the *Napster* court clearly asserted that the *Sony* doctrine rules against imputing knowledge on a service provider—absent specific information identifying infringing activity—just “because the structure of the system allows for the exchange of copyrighted material.”⁵⁹¹

The court next affirmed the District Court's finding that the DMCA requires no less than specific knowledge of particular infringement for the purpose of establishing “actual knowledge.”⁵⁹² “Requiring specific knowledge of particular infringement activity,” the Ninth Circuit maintained, “makes good sense in the context of the DMCA.”⁵⁹³

The court then embarked on a legislative history discussion from which it drew a conclusion that, given the impracticality of requiring OSPs to discern whether or not a material is copyrighted or authorized, the legislative intent appropriately “encourag[e]s copyright holders to identify specific infringing material to service providers.”⁵⁹⁴ The court found additional supports for this conclusion in the notification requirements of the § 512(c)(3)(A) as well as Congress's intention to limit OSPs' responsibility as expressed in § 512(m)(1).⁵⁹⁵ Furthermore, the *UMG III* court reasoned that the notice-centrality aspect of the DMCA—especially the substantial compliance standard under § 512(c)(3)(A)—constitutes an “exclusionary rule” against adducing substantially deficit evidence.⁵⁹⁶ It is this aspect of the DMCA that precludes a court from “determining whether a service provider has actual knowledge or is aware of facts and circumstances from which infringing activity is apparent” based on mere non-specific information of infringement.⁵⁹⁷

Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended at 17 U.S.C.A. § 1201)).

⁵⁹¹ *UMG III*, 667 F.3d at 1037 (quoting *Napster II*, 239 F.3d 1004, 1021 (9th Cir. 2001)).

⁵⁹² *See UMG III*, 667 F.3d at 1035–37 (discussing specific knowledge in the context of knowledge requirements for the safe harbor provision of § 512(c) of the DMCA).

⁵⁹³ *Id.* at 1037.

⁵⁹⁴ *See id.* 1037–38 (noting that copyright holders are the parties that are better equipped to determine when an infringement is occurring, since they know better than the service provider what actually has been copyrighted).

⁵⁹⁵ *Id.*

⁵⁹⁶ *Id.*

⁵⁹⁷ *Id.* at 1037.

b. Apparent Knowledge or Red Flag

Following its discussion of actual knowledge, the *UMG III* court squarely rejected UMG's contention that apparent knowledge under subsection 512(c)(1)(A)(ii) should be subject to a less demanding hurdle than what is required for actual knowledge.⁵⁹⁸ The Ninth Circuit held that *specific knowledge* of infringement must also be the standard upon which red flag awareness is to be applied.⁵⁹⁹ Specifically, the court was not persuaded by the plaintiff's argument that Veoh's mere general awareness of the fact that copyrightable materials are hosted and made available on its system would be sufficient to trigger a red flag.⁶⁰⁰

UMG's theory—that a service provider must sometimes “follow the lead” and initiate investigation on its own—likewise failed to find sympathy from the court.⁶⁰¹ The analysis offered by the court, nonetheless, was rather terse in this respect; the court probably did not want to engage in an argument regarding how the § 512(c) should be interpreted structurally.⁶⁰² In the end, the *UMG III* court only declared its intention to continue adhering to its holding in *CCBill*, which determined that the burden of investigation remains with the copyright holder rather than the service provider.⁶⁰³

Having established that specific knowledge also applies to subsection 512(c)(1)(A)(ii), the court next turned to discuss the adequacy of UMG's evidence demonstrating Veoh's apparent knowledge.⁶⁰⁴ Evidence and records provided by UMG were invariably set aside on various grounds. UMG's first evidence concerned Veoh's purchase of certain “ads words”—search terms allowing a search engine to return results that include links to Veoh—containing names of artists under UMG's control.⁶⁰⁵ The Ninth Circuit, however, did not find such practice to be

⁵⁹⁸ *UMG III*, 667 F.3d at 1038 (“We reach the same conclusion with regard to the § 512(c)(1)(A)(ii) inquiry . . .”).

⁵⁹⁹ *Id.* at 1038–41.

⁶⁰⁰ *Id.* at 1039–40.

⁶⁰¹ *Id.* at 1039.

⁶⁰² *See id.* (noting the brevity of the court's analysis of UMG's purported theory that Veoh should have taken initiative to investigate the materials identified in the notice).

⁶⁰³ *Id.* (citing *CCBill*, 488 F.3d 1102, 1114 (9th Cir. 2007)).

⁶⁰⁴ *UMG III*, 667 F.3d at 1038–40.

⁶⁰⁵ *Id.* at 1038 (pointing to the Veoh's purchase of certain search terms via Google's AdWords program).

dispositive in red flag analysis.⁶⁰⁶ Indeed, the court opined, there can be many reasons why a service provider may want to associate its service with famous artists whose works it is not authorized to use, or with goods or services that the company does not actually provide.⁶⁰⁷ The court offered an example that a company selling shades may want to buy search terms such as “sunscreen” or “vacation” because customers searching around with such terms may also be interested in sunglasses.⁶⁰⁸

UMG fared no better with its evidence comprising of news article, industry reports, and deposition testimony all seeking to establish the point that Veoh was a copyright thief and that it knew of the availability of infringing material under its control.⁶⁰⁹ Among these documents include articles voicing major media companies’ concerns regarding Veoh’s alleged laxity, a fact well known in the industry, in dealing with pirated content.⁶¹⁰ Acknowledgement from Veoh’s CEO, Dmitry Shapiro, concerning copyright problems facing his company was also evident in both news articles and testimonial records.⁶¹¹ The Ninth Circuit, however, remarked that UMG’s evidence was essentially predicated upon the same “general awareness” theory that the court had rejected.⁶¹² The court explained that under the notice-centrality aspect of the DMCA, it is deemed reasonable for a service provider to inadvertently host unauthorized material until it is directed, with adequate information, to take that content down.⁶¹³ According to the *UMG III* court, “[t]he DMCA’s detailed notice and takedown procedure *assumes* that, ‘from time to time,’ ‘material belonging to someone else ends up’ on service providers’ websites, and establishes a process for ensuring the prompt removal of such unauthorized material.”⁶¹⁴

Lastly, the court turned to consider UMG’s evidence comprising of emails sent from third-party copyright holders and

⁶⁰⁶ *Id.* at 1039.

⁶⁰⁷ *Id.*

⁶⁰⁸ *Id.*

⁶⁰⁹ *Id.*

⁶¹⁰ *UMG III*, 667 F.3d at 1039 (pointing to news articles where Veoh was said to be “among[st] the least aggressive video sharing sites in fighting copyrighted content”).

⁶¹¹ *See id.* (Shapiro testified, during deposition testimony, “that he had heard of these articles [cited by *UMG*], and was aware that, ‘from time to time,’ ‘material belonging to someone else ended] up on’ Veoh.”).

⁶¹² *Id.*

⁶¹³ *Id.* at 1039–40.

⁶¹⁴ *Id.*

users. This is, by far, UMG's strongest evidence.⁶¹⁵ The Ninth Circuit openly observed that emails providing details of infringing material from a third party—here from the CEO of Disney to Veoh's investor—are not subject to notice-centrality doctrine of the DMCA. Thus, these emails could constitute a red flag under subsection 512(c)(1)(A)(ii), provided that they are detailed enough to enable a service provider to locate infringing material.⁶¹⁶

Nevertheless, the Ninth Circuit made a reservation that all copyright holders must still be subject to the notification requirements of § 512(c)(3)—regardless of whether or not they are parties to the dispute.⁶¹⁷ Relying on the text of § 512(c)(3)(B)(i), the court held that “[Disney’s] deficient notice ‘shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.’”⁶¹⁸

An email from a non-copyright-holder third party, however, is another matter. Here, UMG produced an email from a user who was displeased with Veoh's refusal to post his unauthorized material and protested against Veoh's decision, claiming that “plenty of [other] copyright infringement material[s]” were allowed to be posted on the site.⁶¹⁹ The *UMG III* court admitted that because this email identified another user who successfully posted infringing content, it could be sufficient to satisfy a red flag test under § 512(c)(1)(A)(ii).⁶²⁰ However, the court observed that because UMG failed to provide evidence that Veoh did not promptly take down the content identified this email by itself would not be sufficient to raise a genuine issue of material fact regarding Veoh's knowledge of infringement.⁶²¹

⁶¹⁵ *Id.* at 1040 (pointing to the fact that UMG comes closer to meeting the requirements of § 512(c)(1)(A) of the DMCA with the email evidence).

⁶¹⁶ *See id.* (“If this notification had come from a third party, such as a Veoh user, rather than from a copyright holder, it might meet the red flag test because it specified particular infringing material.”).

⁶¹⁷ *UMG III*, 667 F.3d at 1040.

⁶¹⁸ *Id.*

⁶¹⁹ *Id.*

⁶²⁰ *Id.*

⁶²¹ *Id.*

c. Willful Blindness and “the Right and Ability to Control”

In its long analysis of the knowledge elements of the DMCA, the Ninth Circuit also addressed UMG’s concern regarding Veoh’s alleged willful blindness practice.⁶²² However, as discussed above, UMG’s weak showing of the nature of deliberate acts allegedly performed by Veoh firmly augmented the court’s confidence that there was no merit in UMG’s willful blindness argument.⁶²³ According to the court:

Viewing the evidence in the light most favorable to UMG . . . we agree with the district court there is no evidence that Veoh acted in such a manner. . . . Although the parties agree, in retrospect, that at times there was infringing material available on Veoh’s services, the DMCA recognizes that service providers who are not able to locate and remove infringing materials they do not specifically know of should not suffer the loss of safe harbor protection.⁶²⁴

Interestingly, the court derived the above conclusion from its analysis on the issue of whether Veoh had “the right and ability to control” infringing activity under § 512(c)(1)(B).⁶²⁵ On this point, UMG argued that the District Court erred when it rejected UMG’s argument that the control element is necessarily met whenever an OSP has “the general ability to locate infringing material and terminate users’ access.”⁶²⁶

In affirming the District Court’s holding on the issue, the Ninth Circuit pointed out that having the legal right and necessary tools to remove infringing content is not the same as having a *practical ability* to control infringing activity — and it is the latter that was on Congress’s mind.⁶²⁷ The court reinforced its hypothesis with extant case law and the basic rule that a statute should be interpreted in accordance with the plain meaning of its text.⁶²⁸ The ordinary meaning of the words “ability” and “control,” the court argued, requires a controlling party —in order that it be competent in the exercise of restraining authority — to be in

⁶²² *Id.* at 1043.

⁶²³ *Supra* notes 579-97 and accompanying text.

⁶²⁴ *UMG III*, 667 F.3d at 1043.

⁶²⁵ *Id.* at 1044.

⁶²⁶ In effect, UMG wanted the court to apply the common law standard of vicarious liability to the DMCA: Service providers would have the “right and ability to control” infringing activity regardless of whether they have knowledge of specific infringing material. *Id.* at 1043.

⁶²⁷ *Id.* at 1043–45.

⁶²⁸ *Id.*

possession of “needed powers . . . or needed resources.”⁶²⁹ In addition, other courts have suggested that service providers must be aware of specific, unauthorized material before they are able to do anything about it.⁶³⁰ Besides, the court remarked, to read the phrase “right and ability to control” in a way suggested by UMG would contravene both § 512(m) and the court’s precedent interpretation of the statute in *CCBill*, which similarly declared that § 512(c) imposes no investigative burden on OSPs.⁶³¹ Consequently, the Ninth Circuit held that “a service provider must be aware of specific infringing material to have the ability to control that infringing activity within the meaning of § 512(c)(1)(B). Only then would its failure to exercise its ability to control deny it a safe harbor.”⁶³²

The *UMG III* court’s conclusion on this issue produced a significant result in the analysis of willful blindness.⁶³³ The consequence of holding that a service provider cannot have the right and ability to control, absent specific knowledge of infringement, appears to suggest that no willful ignorance could be claimed without specific knowledge of the same.⁶³⁴ Note that in this case UMG’s willful blindness claim relied principally on the evidence that Veoh deliberately delayed in implementing Audible Magic filtering technology.⁶³⁵ Instead of engaging in a fruitless debate as to whether a failure to implement filtering technology is relevant in the application of the DMCA, the Ninth Circuit resolved the issue by applying the specific knowledge of infringement requirement across the board.⁶³⁶

d. The DMCA Requirements and Elements under Common Law Secondary Liability Are Not Coextensive

More significantly, and probably the most important point of the decision, the *UMG III* court went on to clarify that the “right and ability to control” element under the DMCA and the common

⁶²⁹ *Id.* at 1041.

⁶³⁰ *UMG III*, 667 F.3d at 1041–42.

⁶³¹ *Id.* at 1042.

⁶³² *Id.*

⁶³³ See discussion *supra* Part 1.3.

⁶³⁴ See *UMG III*, 667 F.3d at 1041 (explaining that a service provider “cannot exercise its ‘power or authority’” over infringing materials “until it becomes aware of specific unauthorized material”).

⁶³⁵ *Id.* at 1028.

⁶³⁶ See *id.* at 1036 (discussing the narrow interpretation the court has taken).

law vicarious liability doctrine, albeit similarly worded, can mean different things in different contexts.⁶³⁷ To this effect, the Ninth Circuit explicitly declined, as per UMG's suggestion, to interpret § 512(c)'s requirements the same way the court had read similar language in the context of common law vicarious liability in *Napster*.⁶³⁸ In reaching this conclusion, the court provided an analysis on three different levels.⁶³⁹

Firstly, the Ninth Circuit deemed a wholesale adoption of the terms as used in vicarious liability jurisprudence to be inappropriate as a practical matter.⁶⁴⁰ There is no statutory mandate, the court noted, that one must apply the DMCA in accordance with a "vicarious liability" standard.⁶⁴¹ Indeed, the vicarious liability elements as applied in common law appear to lack linguistic unity and coherence.⁶⁴² Moreover, contrary to UMG's argument, *Napster* cannot be relied upon as a sole authority in the interpretation of the DMCA.⁶⁴³ The court reasoned that *Napster's* "general ability" doctrine was never codified by Congress and the § 512(c) requires "something more" than mere general ability to locate infringing material and terminate users' access.⁶⁴⁴

On the second level, the court examined the legislative history and concluded that Congress did not intend to deny § 512(c)'s protection to OSPs simply because their operations may subject them to vicarious liability under common law.⁶⁴⁵ The Ninth Circuit was convinced that the drafters of the DMCA envisioned the standards for the statutory safe-harbor to be independent from the judicially developed doctrine of vicarious liability.⁶⁴⁶ As the *UMG III* court put it, "[Congress seeks] to provide safe

⁶³⁷ *Id.* at 1043.

⁶³⁸ *Id.*

⁶³⁹ *Id.* at 1043–45.

⁶⁴⁰ *UMG III*, 667 F.3d at 1043.

⁶⁴¹ *See id.* (noting that "§ 512(c) nowhere mentions the term 'vicarious liability'").

⁶⁴² *See id.* ("the language used in the common law standard is loose and has varied").

⁶⁴³ *Id.* at 1043–44.

⁶⁴⁴ *Id.*

⁶⁴⁵ *Id.* at 1044.

⁶⁴⁶ *UMG III*, 667 F.3d (The court relied on identical passages of legislative reports, discussed above in Part IV, notably the statement that "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.") (quoting S. REP. NO. 105-190, at 19 (1998)).

harbor protection *not* by altering the common law vicarious liability standards, but rather by carving out permanent safe harbors to that liability for Internet service providers even while the common law standards continue to evolve.”⁶⁴⁷

Lastly, on a policy level, the court made an argument that it is inconceivable that Congress would have intended § 512(c) to be entirely parallel to the vicarious liability requirement.⁶⁴⁸ To intend such a result, the court reasoned, would be to “effectively exclude all vicarious liability claims from the § 512(c) safe harbor.”⁶⁴⁹ The court also raised a question of whether it is appropriate to devise a safe harbor system that shields OSPs from one strand of secondary liability while refusing to provide a similar protection against vicarious liability.⁶⁵⁰

The Ninth Circuit concluded its analysis by warning against odd interpretations of the statute absent Congressional guidance.⁶⁵¹ If Congress had intended the result discussed above, the court argued, it likely would have provided a clear statement to that effect.⁶⁵² In fact, that is exactly the case when Congress introduced the law prohibiting an act of circumventing technological protection of copyrighted works, now codified in § 1201 of the Copyright Act.⁶⁵³

3. Case Analysis

a. Actual Knowledge Means Knowledge of *Actual* Infringement

For the most part, the question regarding the existence of actual knowledge will be based on whether a copyright holder has sent a proper DMCA notice to the OSP.⁶⁵⁴ However, while the Court did not explicitly rule out other types of evidence, it

⁶⁴⁷ *Id.*

⁶⁴⁸ *Id.*

⁶⁴⁹ *Id.*

⁶⁵⁰ *Id.*

⁶⁵¹ *Id.* at 1045.

⁶⁵² *UMG III*, 667 F.3d at 1045.

⁶⁵³ *See id.* (Congress stated: “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.”) (quoting 17 U.S.C.A § 1201(c)(2) (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/07/12)).

⁶⁵⁴ *UMG III*, 667 F.3d at 1036 (“UMG’s decision to forego the DMCA notice protocol ‘stripped it of the most powerful evidence of a service provider’s knowledge’”).

provided no alternative examples of evidence that can similarly establish actual knowledge.⁶⁵⁵ On the contrary, the *UMG III* court further excluded non-copyright holder's complaints from the candidacy, even though they might be specific enough for the purpose of locating infringing material.⁶⁵⁶ The court reasoned that such evidence, though specific, would not reveal the infringing nature of the material identified.⁶⁵⁷

It is admittedly difficult to come up with any evidence that contains adequate information to help locate infringing material and, at the same time, also confirm the unauthorized nature of its availability. In practical terms, if such knowledge did not come from a copyright holder, it could only come to light through an OSP's own investigation. One possible example is a service provider's voluntary adoption of filtering technology such as Audible Magic digital fingerprinting software.⁶⁵⁸ Because certain content-filtering technology can reveal the unauthorized nature of an uploaded file, its legal implication may be more drastic than even the "deep-packet" inspection technique, thereby subjecting an OSP to liability because of its own conduct.⁶⁵⁹

Lower courts have already held that the DMCA does not obligate service providers to implement any filtering technology.⁶⁶⁰ However, these tools of content filtering have

⁶⁵⁵ See *id.* at 1036–40 (describing why the specific allegations of actual knowledge in this case did not exist, and failing to provide examples of where it would).

⁶⁵⁶ *Id.* at 1040 & n.14.

⁶⁵⁷ The court remarked that users' complaint would not provide actual knowledge under § 512(c)(1)(A)(i) because users are not in the position to determine whether the material was indeed infringing. *Id.*

⁶⁵⁸ According to the *Myxer Inc.* court's finding, the Audible Magic software can obtain high-level descriptive information about the particular sound recording – including whether the sound recording is owned by a particular record company, and whether the copyright owner seeks to have it blocked from an OSP's Website. *Myxer Inc.*, 2011 U.S. Dist. LEXIS 109668, at *21–22 (C.D. Cal. Apr. 1, 2011).

⁶⁵⁹ See Rob Frieden, *Internet Packet Sniffing and Its Impact on the Network Neutrality Debate and the Balance of Power Between Intellectual Property Creators and Consumers*, 18 *FORDHAM INTELL. PROP. MEDIA & ENT. L.J.* 633, 656 (2008) (arguing that the knowledge acquired from the deep packet inspection practice "will identify significant information about the nature and type of traffic sufficient to put the ISP on actual notice of any copyright infringement").

⁶⁶⁰ See *UMG II*, 665 F. Supp. 2d at 1111 (stating that there is no evidence that the DMCA "imposes an obligation on a service provider to implement filtering technology at all, let alone technology from the copyright holder's preferred vendor"); *Myxer Inc.*, 2011 U.S. Dist. LEXIS 109668 at *88–89

rapidly become standard among service providers hosting musical content.⁶⁶¹ The DMCA's old-fashion takedown mechanism compares poorly with the effectiveness of these content filters which can immediately screen out unauthorized materials very fast and in large numbers.⁶⁶² Their adoption will soon be mandated by the marketplace.⁶⁶³ Until then, it remains an interesting issue whether a service provider would lose its DMCA protection if it ignores the results generated by such filtering tools.⁶⁶⁴

b. "Red Flag" is Still a Meaningful Test for DMCA–Eligibility Determination

While the *UMG III* court's across-the-board application of the "specific knowledge" standard certainly affects how we determine an OSP's apparent knowledge, the Court did maintain that the determination of "red flag" awareness necessarily stays outside the scope of the notice-centrality regime of the DMCA.⁶⁶⁵ This is an important holding in two respects. First, the court made clear that "red flag" still has a significant role in shaping service providers' responsibility under the DMCA.⁶⁶⁶ A service provider can still be disqualified from the DMCA if it ignores certain types of evidence outside proper DMCA notices – provided that they

(explaining that "the DMCA does not place the burden of ferreting out infringement on the service provider"); *but see Fung*, 2009 WL 6355911, at *10 (holding that it was "probative that defendants did not attempt to develop filtering tools or other means of diminishing the use of its products for infringement").

⁶⁶¹ See Peter S. Menell, *Assessing the DMCA Safe Harbors: The Good, the Bad, and the Ugly*, THE MEDIA INSTITUTE (Aug. 31, 2010), <http://www.mediainstitute.org/IPI/2010/090110.php> (explaining that YouTube and Grooveshark use filtering tools for their services).

⁶⁶² Hassanabadi, *supra* note 384, at 438.

⁶⁶³ See Cynthia C. Scott, *Youtube Signs Licensing Deal to Filter Copyright Material on Site*, Yahoo! Voices (Feb. 23, 2007), <http://voices.yahoo.com/youtube-signs-licensing-deal-filter-copyright-material-220957.html> (explaining that the music industry has demanded implementation of content filtering tools as one of the conditions for entering into license deals with many service providers like YouTube).

⁶⁶⁴ While content filters are not currently required by the DMCA, the Court in *Fung* noted the probative value of the defendant's failure to utilize such filtering technology. *Fung*, 2009 WL 6355911, at *10.

⁶⁶⁵ See *UMG III*, 667 F.3d 1022, 1040 (9th Cir. 2011) (discussing third party notifications and whether they would be considered in light of the red flag test, or the notification requirements of the DMCA).

⁶⁶⁶ *Id.*

impart information specific enough to allow the OSP to locate infringing material.⁶⁶⁷ Indeed, the Ninth Circuit relied on its present holding to declare moot UMG's concern that the District Court had conflated the actual knowledge and red flag awareness tests together.⁶⁶⁸ As the *UMG III* court stated:

A user email informing Veoh of infringing material and specifying its location provides a good example of the distinction. Although the user's allegations would not give Veoh actual knowledge under § 512(c)(1)(A)(i), because Veoh would have no assurance that a third party who does not hold the copyright in question could know whether the material was infringing, the email could act as a red flag under § 512(c)(1)(A)(ii) provided its information was sufficiently specific.⁶⁶⁹

Second, under the Ninth Circuit's approach in *UMG III*, the importance of the willful blindness doctrine as an indicator of red flag knowledge is significantly mitigated.⁶⁷⁰ By holding that a non-copyright-owner third party's communication to an OSP could constitute a red flag, if it adequately specified or identified infringing material, the Ninth Circuit thereby rejected the District Court's recommendation that willful blindness is always needed in order to find apparent knowledge based on the red flag test.⁶⁷¹

The main concern, of course, is that the court's categorical rule that all copyright-industry-generated complaints be excluded from red flag analysis might create a free license for an OSP to ignore a whole category of evidence without facing any consequences.⁶⁷² Elsewhere in the opinion the *UMG III* court acknowledged that such willful ignorance may not go unpunished.⁶⁷³ However, it is not clear whether the *UMG III* court intended to reserve willful blindness as an exception to this "exclusionary rule."⁶⁷⁴ The text of the DMCA itself, however,

⁶⁶⁷ *Id.*

⁶⁶⁸ *Id.* at 1039–40.

⁶⁶⁹ *Id.* at 1040 n.14.

⁶⁷⁰ *Id.* at 1043.

⁶⁷¹ *UMG III*, 667 F.3d at 1040; *UMG II*, 665 F. Supp. 2d 1099, 1108 (C.D. Cal. 2009) (holding that "it takes willful ignorance of readily apparent infringement to find a 'red flag'").

⁶⁷² *UMG III*, 667 F.3d at 1040.

⁶⁷³ *See id.* at 1043 (stating that "a service provider cannot willfully bury its head in the sand to avoid obtaining such specific knowledge").

⁶⁷⁴ *See id.* at 1037, 1043 (discussing Congress' inclusion of an "exclusionary rule" and its decision not to extend it to the defendants in this case).

suggests the opposite.⁶⁷⁵ Subsection 512(c)(3)(B)(i) unequivocally declares deficient notifications useless for the purpose of establishing knowledge under § 512(c)(1)(A) and (B) – so long as they come from “a copyright owner.”⁶⁷⁶ The text of the DMCA and its legislative history do not clarify if such term necessarily includes a non-party copyright holder.⁶⁷⁷ But the *UMG III* court downplayed the distinction and considered *all* copyright owners to be subject to the notification requirements.⁶⁷⁸ In this regard, the effect of this categorical ban is likely to be grave on a finding of willful blindness in the context of awareness of infringement raised by third-party notices.⁶⁷⁹

Despite some troubling consequences, the Ninth Circuit’s decision in *UMG III* should be embraced on the following grounds based on this article’s discussion of the role of willful blindness and the determination of red flag awareness.⁶⁸⁰ First, the court’s holding should provide an *ex-ante* incentive for future copyright plaintiffs to produce more concrete evidence of specific infringing material, rather than spending untold hours and substantial resources on claims pertaining to ghost-like information of general awareness, willful blindness, and copyright rogue discourse.⁶⁸¹ This should substantially simplify judicial analysis of red flags, turning it into a more straightforward and less confusing endeavor.⁶⁸² A determination of whether a service provider is eligible for § 512’s safe harbor can now be made mainly on the basis of fundamental notice-and-takedown

⁶⁷⁵ See 17 U.S.C.A. § 512(c)(3) (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/07/12) (stating that a copyright owner can provide notification of infringing material, but if it does not meet the standards in paragraph (1)(A), then the service provider will not be punished for its failure to act).

⁶⁷⁶ *Id.*

⁶⁷⁷ See *id.* (showing how the statute does not include a definition for copyright owner).

⁶⁷⁸ See *UMG III*, 667 F.3d at 1040 (“As a copyright holder, however, Disney is subject to the notification requirements in § 512(c)(3) . . .”).

⁶⁷⁹ See *id.* (inferring that if copyright owners fail to meet the standards under paragraph (1)(A), then third party notices may also fail to meet the standards).

⁶⁸⁰ See *supra* Part IV.C (discussing aspects of the red flag awareness test and the doctrine of willful blindness).

⁶⁸¹ See Dane S. Ciolino & Erin A. Donelon, *Questioning Strict Liability in Copyright*, 54 RUTGERS L. REV. 351, 390 (2002) (contending that “copyright cases are exceedingly complicated, often protracted, and invariably expensive”).

⁶⁸² See Reese, *supra* note 16, at 234 (discussing the “major confusion over the DMCA safe harbors”).

principle.⁶⁸³ Moreover, the *UMG III* court's approach should also prevent copyright plaintiffs from fabricating and augmenting bogus obligations, such as adoption of filtering technology, into the red flag calculus under the DMCA.⁶⁸⁴

Secondly, because the finding of willful blindness is highly contingent on the level of compliance with the DMCA, dissolving the link between apparent knowledge and willful blindness should render more lucid the lower threshold of the DMCA.⁶⁸⁵ This can help lower the DMCA compliance costs borne by OSPs, thus allowing limited-resourced OSPs to stay in and benefit from the § 512(c)'s safe harbor.⁶⁸⁶

Furthermore, the *UMG III* court's new approach in applying the red flag test is inevitable if we are to maintain the integrity of the notice-centrality aspect of the DMCA.⁶⁸⁷ Courts have long struggled to define the role of informal notices coming from third-parties.⁶⁸⁸ In *UMG III*, the Ninth Circuit meets this challenge by adopting a narrower approach of erecting a clear exclusionary rule – in lieu of pursuing a bottomless quest of finding a definitive standard for apparent knowledge.⁶⁸⁹ By adopting a narrower approach, the court guaranteed that a copyright holder may not forego the notice requirements and shift the burden to OSPs by requiring them to respond to all forms of informal complaint.⁶⁹⁰ The *UMG III* court's decision, in this regard, put a decisive stop to the practice disfavored by the *CCBill* court – *viz.* requiring service providers to respond to myriads of defective notices cobbled together by a copyright holder to produce adequate notices.⁶⁹¹

c. Interpretation of DMCA's Requirements Is To Be Made Independently of Common Law Secondary Liability

⁶⁸³ See *UMG III*, 667 F.3d at 1040 (The court's determination that all copyright holders are held to the DMCA's notice requirement removes from the analysis the complex issue of requisite knowledge.).

⁶⁸⁴ See *id.* at 1041–43 (No such duties could be placed upon OSPs, given the court's simplified approach.).

⁶⁸⁵ *Id.*

⁶⁸⁶ *Id.*

⁶⁸⁷ *Id.* at 1037–38.

⁶⁸⁸ See, e.g., *CCBill*, 488 F.3d 1102, 1115 (9th Cir. 2007) (remanding on the issue of third party notices because District Court did not consider potential red flags raised by third parties).

⁶⁸⁹ *UMG III*, 667 F.3d at 1037–38.

⁶⁹⁰ *Id.* at 1038, 1040.

⁶⁹¹ *Id.* at 1040; *CCBill*, 488 F.3d at 1113.

Jurisprudence

Throughout its discussion of the “right and ability to control element,” the court consciously limited the scope of its interpretation of the DMCA around vicarious liability.⁶⁹² The *UMG III* court noticeably refrained from making any suggestion that its analysis may likewise be applied to contributory liability.⁶⁹³ However, there is no reason to conclude that the court’s rationale pertaining to its interpretation of the § 512(c)(1)(B)’s “control” prong of the DMCA should have a limited effect on future interpretations of the DMCA.⁶⁹⁴

The conclusion that some of the DMCA’s requirements cannot be coextensive with the elements of vicarious liability has long been discussed in the academia, albeit with some reservations.⁶⁹⁵ In *UMG III*, the Ninth Circuit made a policy argument — in accord with academics’ concerns—that the only way to maintain the effectiveness of § 512(c)’s safe harbor is to make sure that an OSP cannot be removed from such protection merely because its action satisfies every element of vicarious liability.⁶⁹⁶ Naturally, however, this holding cannot be limited to just the issue of vicarious liability—given that the same public policy applies with equal force in the context of contributory liability.⁶⁹⁷ Essentially, the *UMG III* court’s confirmation of the non-parallel nature of the requirements under two different regimes was simply to reach a conclusion deliberately left out by the District Court in *UMG II*.⁶⁹⁸

⁶⁹² *UMG III*, 667 F.3d at 1041–45.

⁶⁹³ *See id.* at 1045–47 (omitting mention of the DMCA standard in a contributory liability context).

⁶⁹⁴ *Id.* at 1041–45.

⁶⁹⁵ *See Lee, supra* note 277, at 240–42 (asserting that mistakenly treating the DMCA “as though it is identical to the traditional common law standard of vicarious liability” is a “fundamental flaw” in interpreting the statute). Professor Lee, however, thinks that the DMCA only provides OSPs with partial immunity from contributory infringement because an OSP still has to act “expeditiously to remove, or disable access to, the material” in order to remain in the statute’s safe harbor. *Id.* at 248–49.

⁶⁹⁶ *UMG III*, 667 F.3d at 1036–38.

⁶⁹⁷ *See id.* at 1043–45, 1047 (explaining the relationship between contributory, vicarious, and inducement liability).

⁶⁹⁸ *See id.* at 1043, 1045 (reasoning that Congress had not intended “that the § 512(c)(1)(B) ‘right and ability to control’ requirement be coextensive with vicarious liability law); *see supra* notes 531–35 and accompanying text (stating that the court in *UMG II* “did not go far enough as to reach the conclusion that the control element under the DMCA must be construed independently from the common law vicarious liability doctrine”).

What then can explain the Ninth Circuit's apparent reservation against expanding the conclusion reached in its analysis of the right-and-control element of § 512(c)(1)(B) to other parts of the DMCA?⁶⁹⁹ One plausible answer is that the *UMG III* court actually found the standard of knowledge reached under the context of § 512(c) to be in accord with knowledge requirements under contributory infringement jurisprudence.⁷⁰⁰ That, indeed, seemed to be the court's conclusion under its analysis of the plaintiff's claim in *UMG III*.⁷⁰¹

In rejecting the plaintiff's evidence on both actual and apparent knowledge, the *UMG III* court observed that UMG's "general knowledge" theory finds no support even in the secondary liability case law.⁷⁰² As the Ninth Circuit recognized, the Supreme Court in *Sony* had warned against the application of secondary copyright infringement solely on the basis of generalized knowledge.⁷⁰³ The court also pointed out that secondary liability cases in the Internet context, such as *Napster*, had observed the *Sony* Court's admonition and applied, invariably, the standard of specific knowledge of infringement.⁷⁰⁴

In this respect, the *UMG III* court's conclusion apparently deviates from this paper's hypothesis that the DMCA has different knowledge standard from common law indirect liability doctrine.⁷⁰⁵ Nonetheless, there is no reason to think that this divergence should create future uncertainty in the interpretation of the DMCA.⁷⁰⁶ On the contrary, the Ninth Circuit managed, in *UMG III*, to clarify the nature of knowledge required not just under the DMCA but also under common law contributory infringement.⁷⁰⁷ This clarification should discourage future

⁶⁹⁹ *UMG III*, 667 F.3d at 1041–47.

⁷⁰⁰ *See id.* at 1046 (“[O]ne who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a ‘contributory’ infringer.”) (quoting *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 264 (9th Cir. 1996)).

⁷⁰¹ *See id.* at 1046–47 (dismissing UMG's contributory infringement claim because “none of the Investor Directors could individually control Veoh”).

⁷⁰² *Id.* at 1037.

⁷⁰³ *Id.*

⁷⁰⁴ *Id.*

⁷⁰⁵ *See UMG III*, 667 F.3d at 1046 (stating the knowledge standard for contributory infringement, but failing to explain how it differs from that of the DMCA).

⁷⁰⁶ *See id.* at 1043–44 (refusing to interpret the DMCA by common law vicarious liability standards).

⁷⁰⁷ *See id.* at 1043–47 (expounding upon the knowledge requirement in both

copyright plaintiffs from resorting to similar general knowledge/awareness theories, thereby providing a stronger incentive for them to adhere to the notice requirements of the DMCA.⁷⁰⁸

In sum, the *UMG III* court's decision appears to have an unexpected implication that is likely to go beyond the scope of the DMCA.⁷⁰⁹ It is still not clear, however, whether the now-declared-congruent standard of knowledge under the two different regimes would raise a policy concern discussed in the context of vicarious liability: that the DMCA may not provide protection against a contributory liability claim.⁷¹⁰ Nonetheless, given that § 512(c) operates under the notice-centrality regime, which requires more formal specific information, it does not appear that a service provider will lose its safe-harbor protection when knowledge elements under common law contributory liability are met.⁷¹¹

VI. SUGGESTIONS & RECOMMENDATIONS

The application of the DMCA has become more certain in the past few years thanks to a line of cases streaming out from the California and New York District Courts.⁷¹² Although Congress has a strong incentive to stay away from interfering with the contours of judicially developed secondary liability, it should take this chance to update the DMCA in order to get the benefit of judicial interpretation of the safe harbor.⁷¹³ Specifically, it is

contexts).

⁷⁰⁸ *See id.* at 1036–38 (squaring the legislative intent in crafting the DMCA with the Supreme Court's decisions in *Sony* and *Napster* and determining that general knowledge cannot and should not constitute a “red flag” indicator).

⁷⁰⁹ The DMCA requires that service providers have “actual knowledge,” and the Court in *UMG III* defined what that actual knowledge meant, not just for the purpose of the statute, but for the purpose of understanding past rulings. *Id.*; 17 U.S.C.A. § 512(c)(1)(A) (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/07/12).

⁷¹⁰ *See Lee, supra* note 277, at 235 (“Some commentators . . . have suggested that the DMCA contains a loophole that removes vicarious liability from the safe harbors entirely, thereby exposing ISPs to potentially limitless liability for claims of vicarious infringement.”).

⁷¹¹ *Id.* at 240–45 (arguing that the “proper understanding of the DMCA's language . . . is that it establishes partial immunity from vicarious liability”).

⁷¹² *See supra* Part 1.b.1 (discussing *Myxer Inc.* and *Capital Records*); *supra* Part 2.d (discussing *Fung*); *supra* Part IV.B (discussing *Viacom*); *supra* Part V.A (discussing *Io Grp*).

⁷¹³ Since Congress has provided such a loose basis for applying the “red flag” analysis, it would be convenient for it to adopt this tried method as interpreted by the Ninth Circuit specifically; this would respect the separation between the

recommended that the following changes should be made:

First, Congress should codify the Ninth Circuit's interpretation of the DMCA knowledge standard in *UMG III*.⁷¹⁴ This can be done by incorporating new definitions for "actual knowledge" and "apparent knowledge" into the text of § 512—so as to clarify that a "specific knowledge of particular infringing activity" is required to establish either type of knowledge.⁷¹⁵ A similar update should also extend to the "right and ability to control" element under § 512(c)(1)(B).⁷¹⁶ Indeed, the said term should be reworded or rephrased to avoid possible confusion with the similarly worded term under vicarious liability doctrine.⁷¹⁷

Second, Congress should follow the Ninth Circuit approach by revising examples of evidence that can be used as indicators of red flag awareness.⁷¹⁸ The selection of these examples must be made with an understanding that it should reflect the modern expectations of online copyright practice.⁷¹⁹ More significantly, their adducement shall in no way undermine the integrity of the notice-centric aspect of the DMCA or the core principle of the DMCA under § 512(m): that an operator of website should not bear the burden of policing for infringing activities.⁷²⁰

As discussed above, limiting the application of the red flag test on types of evidence is more welcomed than relying on evidence of willful blindness.⁷²¹ Copyright holders should not be encouraged to rely on the defendant's willful ignorance in order to establish apparent knowledge.⁷²² Willful blindness is likely to complicate the application of the DMCA by shifting the focus to OSPs' hidden conscience and attitude toward enforcement of

legislative and judicial branches, while still ensuring that the intricacies of the judicially-created secondary liability doctrine finds its way to codification. *See supra* Part I.

⁷¹⁴ *UMG III*, 667 F.3d at 1036–38.

⁷¹⁵ *Id.* at 1037–38.

⁷¹⁶ *Id.* at 1044.

⁷¹⁷ As the Court discussed in *UMG III*, "Congress did not intend to exclude from § 512(c)'s safe harbor all service providers who would be vicariously liable for their users' infringing activity under the common law." *Id.* at 1044 & n.17.

⁷¹⁸ *Id.* at 1038–41.

⁷¹⁹ *See id.* at 1037 (noting that the DMCA was "enacted to foster cooperation among copyright holders and service providers in dealing with infringement on the Internet").

⁷²⁰ 17 U.S.C.A. §§ 512(c), (m) (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/07/12).

⁷²¹ *See supra* Part II.B.4.

⁷²² *See supra* Part II.B.4.

copyright, thereby making it more expensive for both sides of a dispute and impossible to guarantee a consistent outcome.

In this regard, Congress should consider vesting the Librarian of Congress with the responsibility to conduct research and the rule making authority to incorporate its findings into § 512.⁷²³ For example, it is suggested that the Copyright Office issue a Notice of Proposed Rulemaking and Request for Comments (NPRM) seeking public opinion about what evidence should be appropriate for the purpose of determining apparent knowledge under the DMCA.⁷²⁴

The same approach can also be used to determine whether certain filtering technology should be mandated as a required accommodation for “standard technical measures.”⁷²⁵ The issue of implementation of filtering technology has been repeatedly raised in recent disputes, including *UMG III*.⁷²⁶ Most copyright holders now incorporate into their works content fingerprinting technology for the purpose of identifying and protecting their copyrighted content online.⁷²⁷ OSPs’ accommodation of this technology is rapidly becoming the definitive method for identifying unauthorized uses of copyrighted content in the twenty-first century.⁷²⁸ The DMCA has clearly left open a possibility for new compromises, and fingerprinting technology seems to meet all of the statutory requirements.⁷²⁹ Congress and the Copyright Office, therefore, should initiate a public discussion that will kick-start a development process, compatible with “an open, fair, voluntary, multi-industry standards process” for such technology.⁷³⁰

⁷²³ See Christopher Moseng, *The Failures and Possible Redemption of the DMCA Anticircumvention Rulemaking Provision*, 12 J. TECH. L. & POL’Y 333, 343 (2007) (explaining that the Librarian of Congress was required by the DMCA to determine which classes of copyright works were to be exempt from the statute’s anti-circumvention provision).

⁷²⁴ See *id.* (describing prior NPRMs used to clarify, interpret, and improve upon certain sections of the DMCA).

⁷²⁵ See 17 U.S.C.A. § 512(i) (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/07/12) (“The limitations on liability established by this section shall apply to a service provider only if the service provider . . . accommodates and does not interfere with standard technical measures.”).

⁷²⁶ *E.g.*, *UMG III*, 667 F.3d 1022, 1028 (9th Cir. 2011).

⁷²⁷ Gallo, *supra* note 247, at 296.

⁷²⁸ *Id.* at 296–98.

⁷²⁹ *Id.* at 312.

⁷³⁰ 17 U.S.C.A. § 512 (i)(2)(A) (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/07/12).

With Stop Online Piracy Act (SOPA) being shelved, the content industry will need a more practical and palpable judicial treatment of the red flag knowledge to combat online piracy.⁷³¹ During the recent public opposition against the stalled SOPA, one of the most frequently voiced concerns is that the introduction of the new bill would override the provisions of the DMCA's safe harbors.⁷³² What became apparent is that the once-heavily-criticized DMCA has integrated itself into a common expectation that the public is willing to accept.⁷³³ In this regard, the status of the DMCA, as an engine for online innovation as well as a major tool of enforcement against online piracy, is likely to remain unchanged in the foreseeable future.⁷³⁴

As a cautionary note, Congress should refrain from pursuing any amendment option that would produce undesirable effects on the notice-centrality aspect of the DMCA.⁷³⁵ For instance, in September 2011 the Copyright Office issued an NPRM on the "Designation of Agent to Receive Notification of Claimed Infringement."⁷³⁶ The NPRM basically proposed a new practice regarding the maintenance of designations for the purpose of receiving DMCA notices.⁷³⁷ Failure to comply with the proposed requirements – re-registration plus periodic maintenance of designations – will automatically remove the non-complying OSP from the DMCA safe harbor.⁷³⁸ The new plan implies that a notification of claimed infringement could be communicated via

⁷³¹ John M. Owen, *Graduated Response Systems and the Market for Copyrighted Works*, 27 BERKELEY TECH. L.J. (ANNUAL REVIEW) 559, 579–80 (2012).

⁷³² It is argued that SOPA would bypass the safe harbor provision by placing the responsibility for detecting and policing infringement onto the ISP itself, and allowing judges to block access to websites "dedicated to theft of U.S. property." James Temple, *Stop Online Piracy Act Would Stop Online Innovation*, SFGATE (Nov. 2, 2011, 4:00 AM), <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/11/02/BU881LOIOM.DTL&ao=2>.

⁷³³ *See id.* (discussing the "enormous influence" of the DMCA).

⁷³⁴ *See id.* (explaining the effects of the DMCA on "online innovation, job creation and expression" and asserting that the statute "correctly places the ultimate blame [for copyright infringement] on the infringer, and the onus to police such activity on the copyright holder").

⁷³⁵ 17 U.S.C.A. §§ 512(c), (m) (West, Westlaw through P.L. 112-207 (excluding P.L. 112-199 and 112-206) approved 12/07/12).

⁷³⁶ Designation of Agent To Receive Notification of Claimed Infringement, 76 Fed. Reg. 59,953 (Sept. 28, 2011) (to be codified at 37 C.F.R. pt. 201).

⁷³⁷ *Id.* at 59,953.

⁷³⁸ *Id.* at 59,954–55.

telephone and voice-mail.⁷³⁹ This led to vigorous objection by major OSPs on the ground that it might be used to support the practice of sending takedown requests through voice mails, thereby sidestepping DMCA's written notice requirement.⁷⁴⁰

VII. CONCLUSION

The problem of determining an appropriate knowledge standard has always been a contentious issue in the application of both the secondary liability doctrine and the DMCA's safe harbor. Legislative history and case law, however, suggest that § 512(c) – in order to maintain its effectiveness as a safe harbor – requires a unique standard of interpretation, which must be non-coextensive to the secondary liability doctrine.⁷⁴¹ Nonetheless, earlier DMCA decisions, as well as the legislative history, clearly failed to provide guidance for practical application of “red flag” tests.⁷⁴² The only available means, through a demonstration of willful blindness, will likely turn copyright disputes into wars of words rather than straightforward litigation based on concrete evidence.

The Ninth Circuit's recent holding in *UMG III* managed, to some extent, to reduce ambiguities that have long plagued judicial determinations of the red flag test and re-attuned it to the underlying structure of § 512(c).⁷⁴³ The court achieved a pragmatic reading of the apparent-knowledge prong by making a

⁷³⁹ Specifically, § 201.38(c)(4) of the proposed regulation requires service providers to file: “The physical mail address (street address or post office box), telephone number, and e-mail address of the agent designated to receive notification of claimed infringement” *Id.* at 59,959.

⁷⁴⁰ Specifically, William Patry, acting as senior copyright counsel for Google, Inc., commented,

“We are concerned that the clarifications and the availability of a phone number do not lead to a requirement that service providers designate a specific person to be contacted for voice communication or that leaving of takedown notices be authorized via phone calls or voice mail. Accepting takedown requests via phone or voicemail would present a multitude of problems: for example, lack of documentation to send on to the alleged infringer, lack of signature, problems with verifying identity, detecting abuse, lack of accurate metrics, scalability, and potential differences of opinion about what was identified.”

Letter from William Patry, Senior Copyright Counsel, Google Inc., to Robert Kasunic, Deputy General Counsel, Copyright Office (Nov. 28, 2011), *available at* <http://www.copyright.gov/docs/onlinesp/comments/2011/initial/google.pdf>.

⁷⁴¹ *See supra* Part V.C.2.d.

⁷⁴² *See supra* Part IV.C.1.b.

⁷⁴³ *See supra* Part V.C.3.b–3.c.

much needed clarification on the type of evidence that may constitute a red flag, rather than focusing on the plaintiff's willful blindness and copyright-rogue discourse.⁷⁴⁴ Nevertheless, the DMCA is still replete with other riddles that require attention and interpretation from future courts and, perhaps, some revision from Congress.

The DMCA is now very old in 2012. Online practices, both legal and illegal, concerning consumption and distribution of content have changed tremendously over the last decade. To be sure, much of these changes were made in the likeness and contours of the DMCA. Existing practices that define our online expectations with regard to the use and enjoyment of copyrighted materials largely owed their origin to the scheme set out in the § 512's safe harbors. In this sense, the DMCA has not become entirely obsolete. It merely becomes mature.⁷⁴⁵ Nonetheless, this mature instrument is ripe for revision and it is recommended that Congress take this opportunity to update and accommodate the DMCA for future challenges.

⁷⁴⁴ See *supra* Part V.C.2.b.

⁷⁴⁵ See discussion *supra* Part VI.