

THE RED FLAG TEST FOR APPARENT KNOWLEDGE
UNDER THE DMCA § 512(C) SAFE HARBOR ♦

INTRODUCTION..... 196

I. DIGITAL MILLENNIUM COPYRIGHT ACT SAFE HARBORS..... 198

 A. *The Purpose of the DMCA Safe Harbors*..... 198

 B. *The Safe Harbors of the DMCA* 199

 1. Threshold Requirements Under § 512(i) for
 Safe Harbors..... 199

 2. Requirements Under the § 512(c) Safe
 Harbor 200

II. THE RED FLAG TEST 201

III. JUDICIAL APPLICATION OF THE RED FLAG TEST IS
 INCONSISTENT WITH LEGISLATIVE INTENT 203

 A. *Actual Knowledge Versus Apparent Knowledge* 203

 B. *Alleged Red Flags Are Not Red Enough* 206

 1. Non-Compliant Notices..... 206

 2. Obvious Words of Infringement 209

 3. Password-Hacking Websites 211

 4. Federal Labeling Law Violation 212

 5. Nature of Subject Matter and Professional
 Production..... 213

 6. General Awareness of Infringement..... 214

IV. WHY DO COURTS SEEM RELUCTANT TO FIND APPARENT
 KNOWLEDGE THROUGH THE RED FLAG TEST? 214

 A. *To Promote Internet Development, Free Flow of
 Information, and Electronic Commerce* 215

 1. To Relieve OSPs of the Burden to Investigate 215

 2. To Provide Certainty to OSPs..... 216

 B. *To Place the Burden on the Most Efficient Cost Bearer*..... 217

 C. *To Avoid Higher Costs to Consumers*..... 218

V. AN INSURMOUNTABLE STANDARD FOR FINDING APPARENT
 KNOWLEDGE 219

 A. *Implications of an Insurmountable Standard* 219

♦ Permission is hereby granted for noncommercial reproduction of this Note in whole or in part for education or research purposes, including the making of multiple copies for classroom use, subject only to the condition that the name of the author, a complete citation, and this copyright notice and grant of permission be included in all copies.

B. <i>An Accessible Standard is Necessary to Achieve Congressional Intent</i>	219
CONCLUSION	222

INTRODUCTION

The Internet has played a major role in today's digital age, and websites such as Google.com, Amazon.com, eBay.com, and YouTube.com have become household names. These sites are online service providers ("OSPs")¹ that make possible activities that we enjoy and find convenient such as emailing, purchasing books at a discount, and sharing video clips. While these sites facilitate legitimate activities, they also provide a forum where users and vendors infringe upon others' copyrights by, for example, sharing unauthorized videos or selling bootleg items. In light of this reality and in hopes of recovering from the party with the deeper pockets, copyright holders have sought to hold OSPs liable for their users' infringement. However, holding OSPs liable for third party infringement severely threatens Internet development and electronic commerce because OSPs would be overburdened with liability and legal fees. Conversely, liberating OSPs of all liability also leads to negative results because it would perpetuate infringement and thus discourage copyright holders from creating new works.

In an effort to balance the interests of copyright holders and OSPs in a way that will foster the growth of the Internet, Congress enacted the Digital Millennium Copyright Act ("DMCA") and included safe harbor provisions in § 512(a) through (d).² These safe harbors protect eligible service providers from monetary liability that may arise due to third party copyright infringement, leaving copyright holders with limited injunctive relief.³ This Note analyzes the lack of knowledge requirement under the § 512(c) safe harbor that protects eligible OSPs that store information at the direction of users.⁴ Section 512(c)(1)(A) requires that the OSP lack actual knowledge of its user's infringement or awareness of facts or circum-

¹ As used in § 512, other than in subsection § 512(a), the DMCA defines service provider as a "provider of online services or network access, or the operator of facilities[.]" 17 U.S.C. § 512(k)(1)(B) (2006). For purposes of this Note, the terms "OSP" and "service provider" are used interchangeably.

² S. REP. NO. 105-190, at 1-2 (1998) [hereinafter DMCA S. REP.]. See also *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 665 F. Supp. 2d 1099, 1111 (C.D. Cal. 2009).

³ 17 U.S.C. § 512(a)-(d). See also DMCA S. REP., *supra* note 2, at 20; *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1098-99 (W.D. Wash. 2004).

⁴ 17 U.S.C. § 512(c).

stances from which the infringement is apparent.⁵ Congress created the “red flag test” to assist copyright holders and OSPs in evaluating whether the OSP is aware of such facts or circumstances. In cases where courts have discussed the alleged existence of red flags, courts have referred to awareness of facts or circumstances from which infringement is apparent, as “apparent knowledge” of infringing material.⁶ Accordingly, in a copyright infringement lawsuit, a copyright holder may argue that the OSP has actual knowledge of its user’s infringement or apparent knowledge of its user’s infringement because it is aware of red flags, and therefore, does not qualify for the § 512(c) safe harbor.

In the limited number of cases discussing the red flag test, courts seem reluctant to find apparent knowledge under the red flag test. For instance, although Congress stated that pirate directories “are obviously infringing because they typically use words such as ‘pirate,’ ‘bootleg,’ or slang terms in their URL,”⁷ in *Perfect 10, Inc. v. CCBill LLC* (“*Perfect 10*”), the Ninth Circuit Court of Appeals found that providing services to “illegal.net” and “stolencelebritypics.com” is not a red flag.⁸ Subsequently, in *UMG Recordings, Inc. v. Veoh Networks, Inc.* (“*UMG Recordings*”), the most recent case addressing the red flag test, the District Court for the Central District of California, cited *Perfect 10* and reiterated that “providing services to websites named ‘illegal.net’ and ‘stolencelebritypics.com’ is not enough to raise a ‘red flag’ from which infringing activity is apparent.”⁹ As courts have yet to find facts that rise to the level of apparent knowledge under the red flag test, it is uncertain what circumstances might satisfy the test. These cases leave copyright

⁵ *Id.* See *UMG Recordings*, 665 F. Supp. 2d at 1107; *Corbis*, 351 F. Supp. 2d at 1099.

⁶ The court in *UMG Recordings* used the terms “awareness of facts or circumstances from which infringing activity is apparent” and “apparent knowledge” interchangeably. 665 F. Supp. 2d at 1107. For instance, the court stated that:

Section 512(c)(1)(A) requires that (i) the service provider “not have actual knowledge that the material or an activity using the material on the system or network is infringing”; and (ii) in the absence of actual knowledge, the service provider “is not aware of facts or circumstances from which infringing activity is apparent.” If the service provider did acquire actual or *apparent knowledge*, it must show that it (iii) “act[ed] expeditiously to remove or disable access to the [infringing] material.”

Id. (emphasis added). See also *Corbis*, 351 F. Supp. 2d at 1106 (stating that in order for Amazon, the defendant OSP, to qualify for the safe harbor, “Amazon must show that it does not have actual or *apparent knowledge* that material on its network is infringing.”) (citing 17 U.S.C. § 512(c)(1)(A)(i) & (ii)) (emphasis added).

⁷ H.R. REP. NO. 105-551(II), pt. 2, at 58 (1998) [hereinafter DMCA H.R. REP.].

⁸ *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1114 (9th Cir. 2007), *cert. denied*, 552 U.S. 1062 (2007).

⁹ *UMG Recordings*, 665 F. Supp. 2d. at 1111 (citing *Perfect 10*, 488 F.3d at 1114).

holders doubting whether it is ever possible to establish the OSP's apparent knowledge under the red flag test.

The purpose of this Note is to discuss how courts have made it practically impossible for a copyright owner to establish apparent knowledge under the red flag test, and how an accessible standard for the red flag test is necessary to achieve the purpose of the DMCA. Part I provides a brief summary of the DMCA's purpose and safe harbors. Part II defines the red flag test. Part III explores whether judicial application of the red flag test is inconsistent with legislative intent. Part IV discusses the possible reasons why courts have been reluctant to find apparent knowledge under the red flag test. Part V explains the implications of setting an insurmountable standard for the red flag test and how an accessible standard is necessary to achieve the DMCA's purpose.

I. DIGITAL MILLENNIUM COPYRIGHT ACT SAFE HARBORS

A. *The Purpose of the DMCA Safe Harbors*

In 1998, Congress enacted the DMCA "to facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age."¹⁰ The DMCA was designed to address "unique copyright enforcement problems caused by the widespread use of the [I]nternet."¹¹ Congress created safe harbors under the DMCA to motivate both the creation of new works and the rapid growth of various industries on the Internet while limiting the unconstrained liability that an OSP might face due to its users' actions.¹² These limitations, listed under § 512(a) through (d), protect eligible service providers from monetary liability, leaving the plaintiff with limited injunctive relief, when services are used to infringe copyrights.¹³

In addition to providing OSPs greater certainty regarding their liability due to third party infringements,¹⁴ the DMCA safe harbors balance the interests of copyright holders and OSPs by creating strong incentives for them "to cooperate to detect and deal with copyright infringements that take place in the digital networked environment."¹⁵ Specifically, to qualify for the § 512(c) safe harbor, the OSP must act expeditiously to

¹⁰ DMCA S. REP., *supra* note 2, at 1-2.

¹¹ *Corbis*, 351 F. Supp. 2d at 1098.

¹² DMCA H.R. REP., *supra* note 7, at 49-50.

¹³ DMCA S. REP., *supra* note 2, at 20.

¹⁴ DMCA H.R. REP., *supra* note 7, at 49-50; DMCA S. REP., *supra* note 2, at 20.

¹⁵ DMCA H.R. REP., *supra* note 7, at 49; DMCA S. REP., *supra* note 2, at 20.

remove or disable access to the infringing material once it acquires knowledge of the infringement.¹⁶ The DMCA also includes a “notice and take-down” mechanism, which calls for the copyright holder to notify the OSP of the infringement according to § 512(c)(3), and requires the OSP to act expeditiously to remove or disable access to the infringing material.¹⁷ The DMCA places the burden on the copyright holder to police potential infringing activities,¹⁸ and upon proper notification, on the OSP to reasonably implement a termination policy in order to qualify for the safe harbors.¹⁹

B. *The Safe Harbors of the DMCA*

Section 512 of the DMCA has four safe harbors that protect the service provider from monetary damages that may arise due to direct, vicarious, and contributory copyright infringement.²⁰ These safe harbors provide protection for four types of service provider activities: (a) maintaining transitory digital network communications, (b) system caching, (c) storing information on the systems or networks at the direction of users, and (d) containing information location tools.²¹ These safe harbors are not intended to alter existing principles of copyright law.²² They only protect service providers from monetary liability. To qualify for a safe harbor, the OSP must be a service provider as defined in § 512(k)²³ and meet the threshold requirements under § 512(i) as well as the specific requirements under one of the § 512(a) through (d) safe harbors.

1. Threshold Requirements Under § 512(i) for Safe Harbors

Section 512(i)(1) lists two conditions for eligibility: (A) the OSP must have adopted and reasonably implemented a policy for termination of repeat infringers; and (B) the OSP must not interfere with standard technical measures.²⁴ The first requirement is relevant to the discussion of the red flag

¹⁶ 17 U.S.C. § 512(c)(1)(A).

¹⁷ 17 U.S.C. § 512(c)(1)(C). *See also* *Ellison v. Robertson*, 357 F.3d 1072, 1076 (9th Cir. 2004).

¹⁸ *Perfect 10*, 488 F.3d at 1113.

¹⁹ 17 U.S.C. § 512(i). *See also* *Ellison*, 357 F.3d at 1080.

²⁰ DMCA H.R. REP., *supra* note 7, at 50; DMCA S. REP., *supra* note 2, at 20. *See also* *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1142 (N.D. Cal. 2008); *Corbis*, 351 F. Supp. 2d at 1098-99.

²¹ 17 U.S.C. § 512(a)-(d).

²² DMCA H.R. REP., *supra* note 7, at 50; DMCA S. REP., *supra* note 2, at 19.

²³ For purposes of § 512(c), a service provider is a “provider of online services or network access, or the operator of facilities[.]” 17 U.S.C. § 512(k)(1)(B).

²⁴ 17 U.S.C. § 512(i)(1).

test because the standards for both a reasonably implemented policy and the red flag test involve a determination of whether the OSP has knowledge of the infringement. A policy is unreasonably implemented if the OSP fails to respond when it has knowledge of the infringement.²⁵ To determine whether the OSP has knowledge, some courts apply the § 512(c) knowledge standard, which includes the red flag test under § 512(c)(1)(A)(ii).²⁶

2. Requirements Under the § 512(c) Safe Harbor

In order to qualify for the § 512(c) safe harbor, the OSP must lack knowledge of the infringement,²⁷ not receive financial benefit from the infringing activity,²⁸ respond expeditiously to remove or disable access to the infringing material upon notification,²⁹ and have a designated agent to receive notifications.³⁰

The lack of knowledge requirement under § 512(c)(1)(A) states that

A service provider shall not be liable for monetary relief . . . if the service provider—

- (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
- (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
- (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material[.]³¹

Thus, a service provider will not qualify for the safe harbor if it has (i) actual knowledge of the infringement, or (ii) apparent knowledge³² of the infringement unless (iii) it acts expeditiously to remove the infringing material. To establish actual knowledge, a copyright holder may provide the OSP's designated agent with a notification that substantially complies

²⁵ *Perfect 10*, 488 F.3d at 1109.

²⁶ *Id.* at 1113-14.

²⁷ 17 U.S.C. § 512(c)(1)(A). Sections 512(c) and (d) have the same lack of knowledge requirement. *See* 17 U.S.C. § 512(c)-(d). Congressional reports have referred to both § 512 (c) & (d) as red flag tests. *See* DMCA H.R. REP., *supra* note 7, at 53, 57; DMCA S. REP., *supra* note 2, at 44, 49.

²⁸ 17 U.S.C. § 512(c)(1)(B).

²⁹ 17 U.S.C. § 512(c)(1)(C).

³⁰ 17 U.S.C. § 512(c)(2).

³¹ 17 U.S.C. § 512(c)(1)(A). *See also* 17 U.S.C. § 512(d)(1).

³² *See supra* note 6.

with § 512(c)(3).³³ Alternatively, a copyright holder may present evidence that the OSP has apparent knowledge of the infringement under the red flag test, that is, that the OSP is aware of circumstances from which infringement is apparent.³⁴

Receipt of a proper notification of infringement from the copyright holder constitutes the OSP's actual knowledge.³⁵ Although receipt of a defective notice cannot establish the OSP's actual knowledge, a notice that *substantially* complies with the statutory requirements of § 512(c)(3)(A) is evidence of the OSP's apparent knowledge.³⁶ The DMCA provides that if the notice complies with 512(c)(3)(A)(ii)-(iv), then the notice will be considered to determine the OSP's knowledge, unless the OSP takes prompt action of removal.³⁷ However, a non-compliant notice plays no role in the analysis of the red flag test for apparent knowledge³⁸ in that "neither the fact that the copyright owner sent the notice nor anything in the content of the notice" is used to determine the OSP's knowledge.³⁹

In sum, the OSP does not qualify for the §512(c) safe harbor if it has actual knowledge of the infringing material or apparent knowledge of the infringing material as established under the red flag test, unless it acts expeditiously to remove the infringing material.⁴⁰

II. THE RED FLAG TEST

The red flag test is a tool that Congress created to assist copyright holders and OSPs in evaluating whether the OSP has apparent knowledge of its user's infringement, and thus, may not qualify for the § 512(c) safe harbor. The legislative record labels § 512(c)(1)(A)(ii) as a "red flag test" consisting of two prongs.⁴¹ The first prong, which has a subjective component,

³³ *Corbis*, 351 F. Supp. 2d at 1107.

³⁴ DMCA H.R. REP., *supra* note 7, at 53, 57; DMCA S. REP., *supra* note 2, at 44, 49.

³⁵ *Corbis*, 351 F. Supp. 2d at 1107 (citing 3-12B MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT, § 12B.04[A][3] (2009)).

³⁶ *Corbis*, 351 F. Supp. 2d at 1108 (citing 17 U.S.C. § 512(c)(3)(B)(i) and *ALS Scan, Inc. v. RemarQ Comties., Inc.*, 239 F.3d 619, 625 (4th Cir. 2001)).

³⁷ See 17 U.S.C. § 512(c)(3)(B)(ii).

³⁸ According to 17 U.S.C. § 512(c)(3)(B)(i),

Subject to clause (ii), 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.

³⁹ Todd E. Reese, *Wading Through the Muddy Waters: The Courts' Misapplication of Section 512(c) of the Digital Millennium Copyright Act*, 34 SW. U. L. REV. 287, 301 (2004).

⁴⁰ See *Io Group*, 586 F. Supp. 2d at 1146.

⁴¹ "[S]ubsection [§ 512](c)(1)(A)(ii) can best be described as a 'red flag' test . . . [which] has both a subjective and an objective element." DMCA H. REP., *supra* note 7, at 53; DMCA, *supra* note 2, at 44.

determines *whether the OSP is aware of the circumstances of infringement*.⁴² The second prong, which has an objective component, determines *whether the infringement is apparent from the circumstances*, that is, “whether infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances.”⁴³ The subjective prong addresses the OSP’s awareness of the alleged red flag, while the objective prong completes the test by addressing whether the alleged red flag is sufficiently apparent to a reasonable person in a similar position as the OSP. The OSP has apparent knowledge of its user’s infringement under the red flag test if both prongs are met, that is, if (1) the OSP is aware of the circumstances related to the infringement, and (2) the infringement is apparent from the circumstances.

Congress created the two-part structure for the red flag test to ensure that an OSP is not burdened with the duty to monitor its services or to affirmatively investigate circumstances indicating infringing activity.⁴⁴ Through the inclusion of a subjective component into the red flag test, Congress distinguished apparent knowledge from constructive knowledge. Accordingly, the court in *Corbis Corp. v. Amazon.com, Inc.* (“*Corbis Corp.*”) interpreted § 512(c)(1)(A)(ii) as requiring apparent knowledge rather than constructive knowledge.⁴⁵ In this case, the copyright holder brought a copyright infringement action against Amazon, the OSP, arguing that Amazon did not qualify for the safe harbor because it *should have known* that its vendors sold infringing material.⁴⁶ The court held that Amazon qualified for the § 512(c) safe harbor, and explained that the question is not what a reasonable person would have deduced from the circumstances.⁴⁷ Instead, the question under § 512(c)(1)(A)(ii) is “whether the service provider deliberately proceeded in the face of blatant factors of which it was aware”⁴⁸ or whether it turned a blind eye to red flags of obvious infringement.⁴⁹ Under the subjective standard, it is not enough that the OSP should have known about the infringement; the OSP has apparent knowledge only if it is aware of the circumstances that indicate apparent infringement.

⁴² DMCA H. REP., *supra* note 7, at 53; DMCA S. REP., *supra* note 2, at 44.

⁴³ DMCA H. REP., *supra* note 7, at 53; DMCA S. REP., *supra* note 2, at 44.

⁴⁴ DMCA H. REP., *supra* note 7, at 53; DMCA S. REP., *supra* note 2, at 44.

⁴⁵ *Corbis*, 351 F. Supp. 2d at 1108.

⁴⁶ *Id.* at 1107 (emphasis added).

⁴⁷ *Id.* at 1108.

⁴⁸ *Id.*

⁴⁹ *Id.* (citing DMCA H. REP., *supra* note 7, at 57).

III. JUDICIAL APPLICATION OF THE RED FLAG TEST IS INCONSISTENT WITH LEGISLATIVE INTENT

To this day, apparent knowledge has never been found through the red flag test. Indeed, it seems impossible for the copyright holder to establish knowledge unless the OSP receives notice according to the statutory requirements. In cases discussing the red flag test, courts have reached results that are inconsistent with legislative intent, such as conflating actual knowledge with apparent knowledge, discouraging OSPs from cooperating with copyright owners, and ignoring legislative directives.

A. *Actual Knowledge Versus Apparent Knowledge*

The standard for the subjective prong of the red flag test is one of actual knowledge of the *circumstances* from which infringement is apparent,⁵⁰ rather than actual knowledge of the infringement itself. However, in *Perfect 10* and in *Io Group, Inc. v. Veoh Networks, Inc.* (“*Io Group*”), both courts essentially required the OSP to have actual knowledge of the infringement rather than of the circumstances of apparent infringement.

In *Perfect 10*, plaintiff Perfect 10 brought a suit against defendants CCBill and CWIE for providing services to “illegal.net” and “stolencelebritypics.com,” websites that posted images that infringed upon Perfect 10’s copyright.⁵¹ Perfect 10 argued that the defendants did not qualify for the DMCA safe harbors because they were aware of red flags that signaled apparent infringement.⁵² Perfect 10 alleged that the defendants must have been aware of the apparent infringing activity due to the illicit website names.⁵³ However, the court concluded that the website names were not a red flag because “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.”⁵⁴ The court reasoned the OSPs do not have the burden to determine whether the photographs were *actually* infringing.⁵⁵ However, under § 512(c), the OSP does not qualify from the safe harbor if it has awareness of “facts or circumstances from which infringing activity is *apparent*.”⁵⁶ In other words, if the OSP is

⁵⁰ 17 U.S.C. § 512(c)(1) (emphasis added).

⁵¹ *Perfect 10*, 488 F.3d at 1107, 1114.

⁵² *Id.* at 1114.

⁵³ *Id.*

⁵⁴ *Id.*

⁵⁵ *Id.* (emphasis added). See *Io Group*, 586 F. Supp. 2d at 1149.

⁵⁶ 17 U.S.C. § 512(c)(1)(A)(ii). If the OSP obtains knowledge, then it must act expe-

aware of facts of *apparent* infringement, then it is not eligible for the safe harbor, unless it acts expeditiously to remove the infringing material, even though the OSP does not know whether there is actual infringement. In spite of the statutory language, the court in *Perfect 10* raised the standard to find apparent knowledge under the red flag test. The court seemed to require the OSP to know that the photographs were actually infringing even though the statute only requires awareness of facts from which infringement is *apparent* to the OSP. Thus, under the court's interpretation that a particular circumstance is not a red flag because the OSP has no burden to determine whether there is actual infringement, the red flag test is effectively dead. If the OSP had knowledge that the photographs were *actually* infringing, then the OSP would have actual knowledge.

The court also conflated apparent knowledge with actual knowledge in *Io Group*. Plaintiff Io Group owned copyrights to ten films that were illegally posted on defendant's website.⁵⁷ The issue was whether the § 512(c) safe harbor applied to Veoh⁵⁸ for providing the forum where its users shared infringing files over the Internet.⁵⁹ The court held that Veoh qualified for the § 512(c) safe harbor because it had no knowledge of the infringement and granted Veoh's motion for summary judgment.⁶⁰

In discussing the lack of knowledge requirement, the court held that Veoh had no actual knowledge since Io Group never notified Veoh.⁶¹ Arguing that Veoh had apparent knowledge, Io Group alleged the following as red flags of obvious infringement: (1) its trademark that appeared in one of the videos that Veoh's user uploaded, (2) the professional and sexually explicit nature of the video clips, and (3) Veoh's user's failure to label the videos as mandated by federal law.⁶² The court analyzed the three alleged red flags separately. First, "there was no evidence from which it can be inferred that Veoh was aware of, but chose to ignore [plaintiff's trademark]."⁶³ Second, the nature of the clips was not a red flag.⁶⁴ Third, the court stated that the OSP's potential awareness of

ditiously to remove or disable access to the infringing material in order to be eligible to the § 512(c) safe harbor. 17 U.S.C. § 512(c)(1)(A)(iii).

⁵⁷ *Io Group*, 586 F. Supp. 2d at 1136.

⁵⁸ *Id.* at 1146.

⁵⁹ *Id.* at 1136.

⁶⁰ *Id.* at 1155.

⁶¹ *Id.* at 1148.

⁶² *Id.* at 1148-49.

⁶³ *Io Group*, 586 F. Supp. 2d at 1149.

⁶⁴ *Id.*

the violation of a federal labeling law did not raise a genuine issue of material fact regarding knowledge of infringement.⁶⁵

Viewing the facts in light most favorable to the copyright holder, the court should have denied the OSP's motion for summary judgment.⁶⁶ The court found that there was a question of fact as to whether Veoh was aware of the federal labeling laws violation.⁶⁷ Such possibility, coupled with Veoh's awareness of the sexually explicit nature of the videos, should have been sufficient to raise a genuine issue of material fact as to whether the OSP was aware of circumstances of apparent infringement. Holding that the red flag test was not satisfied, when the OSP may have been aware of circumstances from which infringement may be apparent, the court conflated apparent knowledge with actual knowledge. The court's interpretation of the red flag test seemed to require Veoh to have actual knowledge of the infringement itself (user was not authorized to upload video) rather than of the circumstances (user violated federal labeling laws) from which one may infer that the uploading user was not the authorized producer of the sexually explicit videos.⁶⁸

As a result of suggesting that the red flag test cannot be satisfied without first proving actual knowledge, the courts' interpretation was inconsistent with the purpose of the red flag test, which is to impute apparent knowledge, absent actual knowledge, where the OSP was aware of circumstances from which infringement is apparent. This judicial interpretation of apparent knowledge was also inconsistent with the DMCA's statutory text because actual knowledge and apparent knowledge are two distinct concepts as they are found in separate provisions under § 512(c)(1).⁶⁹ Thus, in both cases, the court blurred the line between actual knowledge and apparent knowledge, rendering § 512(c)(1)(A)(ii),⁷⁰ the language regarding apparent knowledge, superfluous.

⁶⁵ *Id.*

⁶⁶ Summary judgment is proper only if the evidence "show[s] that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." FED. R. CIV. P. 56(c). During summary judgment, the court examines evidence in light most favorable to the non-moving party. *Corbis*, 351 F. Supp. 2d at 1097 (citing *U.S. v. Diebold, Inc.*, 369 U.S. 654, 655 (1962)).

⁶⁷ *Id. Group*, 586 F. Supp. 2d at 1149.

⁶⁸ *Id.*

⁶⁹ Section 512(c)(1)(A)(i) refers to actual knowledge and § 512(c)(1)(A)(ii) refers to apparent knowledge. 17 U.S.C. § 512(c)(1)(A)(i)-(ii).

⁷⁰ Section 512(c)(1)(A)(ii) requires that "in the absence of . . . actual knowledge, [the OSP] is not aware of facts or circumstances from which infringing activity is apparent . . ." 17 U.S.C. § 512(c)(1)(A)(ii).

B. *Alleged Red Flags Are Not Red Enough*

The following case law shows that courts have made it virtually impossible for copyright holders to establish the OSP's apparent knowledge of infringement through the red flag test. Copyright holders have argued in numerous cases that OSPs were aware of red flags, and therefore, did not qualify for the § 512(c) safe harbor. Yet, notwithstanding the obviousness of the infringement, courts have consistently held that the alleged red flag was not sufficiently evident for a reasonable person to find the copyright infringement apparent. As a result, courts seemed to be disregarding legislative intent in terms of providing a means for copyright owners to hold OSPs accountable for instances where the OSP is aware of "facts and circumstances from which infringing activity is apparent,"⁷¹ yet actual knowledge cannot be established.

1. Non-Compliant Notices

Although the DMCA states that a noncompliant notice that substantially complies with the statutory requirements of § 512(c)(3)(A) may be a red flag,⁷² the following cases show that courts are reluctant to find a notification substantially compliant with the statute.

In *Hendrickson v. eBay Inc.*, the issue was whether eBay can be held secondarily liable for providing a forum to sellers of infringing copies of the movie *Manson*.⁷³ Hendrickson, owner of the copyright in the movie, sent a letter to eBay stating that pirated copies of the movie were being offered for sale on eBay⁷⁴ and alleged that its notice provided eBay with knowledge. The court held that eBay had no actual knowledge or awareness of apparent infringing activity.⁷⁵

The court found that the plaintiff's notifications did not comply with the elements of notification under § 512(c)(3)(A)(ii)-(iv) because the plaintiff did not properly identify the listings of unauthorized copies of the movie, and therefore failed to comply with §512(c)(A)(ii).⁷⁶ In addressing the identification requirement under § 512(c)(3)(A), the court stated that "there may be instances where a copyright holder need not provide [the OSP] with specific item numbers

⁷¹ 17 U.S.C. § 512(c)(1)(A)(ii).

⁷² 17 U.S.C. § 512(c)(3)(B)(ii). See *Corbis*, 351 F. Supp. 2d at 1108 (citing 17 U.S.C. § 512(c)(3)(B)(i) and *ALS Scan*, 239 F.3d at 625).

⁷³ *Hendrickson v. eBay Inc.*, 165 F. Supp. 2d 1082, 1087 (C.D. Cal. 2001).

⁷⁴ *Id.* at 1084.

⁷⁵ *Id.* at 1093.

⁷⁶ *Id.*

to satisfy the identification requirement.”⁷⁷ Instead, where the movie has not been released, it is sufficient “if a movie studio advised [the OSP] that *all* listings offering to sell a new movie . . . are unlawful.”⁷⁸ Here, Hendrickson argued that he notified eBay over a telephone conversation that all copies of the movie are unauthorized.⁷⁹ However, the court concluded that the plaintiff failed to provide eBay with sufficient information on how to distinguish an authorized copy of the movie from an unauthorized one because the notice was not in writing.⁸⁰

In the later case of *Hendrickson v. Amazon.com, Inc.*, Hendrickson notified Amazon in writing that he was the copyright owner of all copies of the unreleased movie *Manson*, and that *all* copies of the movie are infringing because it has not been released yet.⁸¹ Approximately ten months after sending the notice, Hendrickson brought suit against Amazon for direct and vicarious copyright infringement after purchasing an unauthorized copy of *Manson* on Amazon.⁸² The court affirmed the lower court’s summary judgment in favor of Amazon on the direct infringement claim because Amazon was not the actual seller.⁸³ On the issue of vicarious liability, Amazon asserted the safe harbor affirmative defense under § 512(c).⁸⁴ Notwithstanding the fact that the plaintiff notified Amazon that all copies are infringing and the *Hendrickson v. eBay Inc.* opinion,⁸⁵ the court held that the lack of knowledge and awareness criteria under § 512(c)(1)(A) were satisfied.⁸⁶ The court reasoned that Hendrickson’s notification did not substantially comply with the statute because the notification must refer to an infringing activity occurring at the time the OSP receives notice and is not valid for future infringement. Here, Hendrickson sent a notification to Amazon before the infringing activity took place.⁸⁷ The court distinguished *eBay*’s reasoning and explained that the language in the DMCA is in present tense,⁸⁸ and therefore, a blanket notice would only be valid for

⁷⁷ *Id.* at 1090.

⁷⁸ *Id.* at 1090.

⁷⁹ *eBay*, 165 F. Supp. 2d at 1090-91.

⁸⁰ *Id.*

⁸¹ *Hendrickson v. Amazon.com, Inc.*, 298 F. Supp. 2d 914, 915 (C.D. Cal. 2003).

⁸² *Id.*

⁸³ *Id.*

⁸⁴ *Id.*

⁸⁵ “[A] copyright holder need not provide eBay with specific item numbers . . . if a movie studio advised eBay that *all* listings offering to sell a new movie . . . are unlawful . . .” *eBay*, 165 F. Supp. 2d at 1090 (emphasis added).

⁸⁶ *Hendrickson v. Amazon.com, Inc.*, 298 F. Supp. 2d at 918.

⁸⁷ *Id.* at 917.

⁸⁸ According to the DMCA,

[A] notification from a copyright owner that fails to comply substantially with §

currently infringing material and not for future infringement.⁸⁹

The holdings in *Hendrickson v. eBay Inc.* and *Hendrickson v. Amazon.com, Inc.* frustrate the purpose of Congress because they discourage OSPs from cooperating with copyright holders in detecting and dealing with infringement on the Internet.⁹⁰ If a notice stating that all copies are unauthorized is valid only for currently infringing material, then the court provides no incentive for the OSP to monitor its services or take any other action after it runs an initial search. The OSP would not be on notice for infringement occurring after that initial search, and therefore, would not have knowledge of any subsequent listing of an unauthorized copy.

Additionally, *Perfect 10* further shows judicial reluctance to find a notice substantially compliant with § 512(c)(3). In that case, plaintiff Perfect 10 provided defendants CCBill and CWIE with notifications regarding the infringing material.⁹¹ Despite the fact that the OSPs' designated agent admitted that he could have found the infringing photographs based on one of the notifications,⁹² the court refused to impute apparent knowledge of the infringement upon the defendants because the notification lacked a certification under penalty of perjury,⁹³ as required under § 512(c)(3)(A)(vi).⁹⁴ The notices were not considered under the red flag test because they did not sufficiently comply with all the notice requirements under § 512(c)(3).⁹⁵ However, under § 512(c)(3)(B)(ii), a notice that complies with § 512(c)(3)(A)(ii), (iii) and (iv) is used to determine the OSP's knowledge unless the OSP "promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of [a substantially compliant] notification."⁹⁶ Yet, according to the court's inter-

512(c)(3) "shall not be considered under [the first prong of the safe harbor test] in determining whether a service provider has actual knowledge or is aware of the facts or circumstances from which infringing activity is apparent."

Id. at 917-18 (quoting 17 U.S.C. § 512(c)(3)(B)(i)-(ii)).

⁸⁹ *Id.* at 917.

⁹⁰ The purpose of the DMCA safe harbors is to encourage copyright holders and OSPs to cooperate in detecting and dealing with copyright infringements. DMCA H. REP., *supra* note 7, at 49; DMCA S. REP., *supra* note 2, at 20.

⁹¹ *Perfect 10*, 488 F.3d at 1111-12.

⁹² Opening Brief of Plaintiff-Appellant at 12, *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, No. 04-57143, 04-57207 (9th Cir. Mar. 24, 2005). See also NIMMER & NIMMER, *supra* note 35, § 12B.04[B][4][c].

⁹³ *Perfect 10*, 488 F.3d at 1112.

⁹⁴ Section 512(c)(3)(A)(vi) requires a statement under penalty of perjury that the complaining party is authorized to represent the copyright holder and that infringement is taking place. 17 U.S.C. § 512(c)(3)(A)(vi).

⁹⁵ *Perfect 10*, 488 F.3d at 1111-12.

⁹⁶ According to 17 U.S.C. § 512(c)(3)(B)(ii),

In a case in which the notification that is provided to the service provider's desig-

pretation of the statute, “substantial compliance means substantial compliance with *all* of § 512(c)(3)’s clauses, not just some of them.”⁹⁷ Thus, rather than focusing on whether the OSPs acted reasonably to assist in the receipt of a substantially compliant notification, the court found that a notice is not substantial if it complies with only some of the requirements of § 512(c)(3)(A).⁹⁸

2. Obvious Words of Infringement

Congress explained that sites with “words such as ‘pirate,’ ‘bootleg,’ or slang terms in their URL” are obviously infringing, and that “safe harbor status for a provider that views such a site . . . would not be appropriate”⁹⁹ because “the infringing nature of such sites would be apparent from even a brief and casual viewing.”¹⁰⁰ In other words, slang words such as “pirate” and “bootleg” are red flags because infringement is apparent from a brief and casual viewing.¹⁰¹ Although the court in *Corbis Corp.* embraced the legislature’s explanation, subsequent cases rejected Congress’s instructions in addressing suspicious website names. The court in *Perfect 10* acted in direct conflict with legislative directives while addressing the use of suspicious website names when it found, and other courts reiterated,¹⁰² that providing services to “illegal.net” and “stolencelebritypics.com” is not a red flag.¹⁰³

In *Corbis Corp.*, the court stated that “a copyright owner could establish apparent knowledge if she could show that an online location at which her copyrighted material was available

nated agent fails to comply substantially with all the provisions of subparagraph (A) but substantially complies with clauses (ii), (iii), and (iv) of subparagraph (A), clause (i) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions of subparagraph (A).

Clause (i) of this subparagraph states,

Subject to clause (ii), 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.

17 U.S.C. § 512(c)(3)(B)(i).

⁹⁷ *Perfect 10*, 488 F.3d at 1112.

⁹⁸ *Id.*

⁹⁹ DMCA H. REP., *supra* note 7, at 58; DMCA S. REP., *supra* note 2, at 48.

¹⁰⁰ DMCA H. REP., *supra* note 7, at 58; DMCA S. REP., *supra* note 2, at 48.

¹⁰¹ *Corbis*, 351 F. Supp. 2d at 1108.

¹⁰² “The Ninth Circuit has concluded that even providing services to websites named ‘illegal.net’ and ‘stolencelebritypics.com’ is not enough to raise a ‘red flag’ from which infringing activity is apparent.” *UMG Recordings*, 664 F. Supp. 2d at 1111 (citing *Perfect 10*, 488 F.3d at 1114). See also *Io Group*, 586 F. Supp. 2d at 1149.

¹⁰³ *Perfect 10*, 488 F.3d at 1114.

was clearly a ‘pirate site.’”¹⁰⁴ Websites that use words such as “pirate” and “bootleg” in their URL make their illegal purpose obvious, and their infringing nature would be apparent from even a mere look.¹⁰⁵ Therefore, once the OSP is aware of such site, the OSP would have apparent knowledge of the infringing activity.¹⁰⁶ Still, less than three years later in *Perfect 10*, the Ninth Circuit Court of Appeals stated that using terms such as “illegal” might just be an attempt to attract clients.¹⁰⁷

Despite congressional reports stating that pirate sites constitute red flags,¹⁰⁸ the Ninth Circuit Court of Appeals in *Perfect 10* rejected the websites “illegal.net” and “stolencelebritypics.com” as red flags. Plaintiff Perfect 10 argued that the defendants were not eligible for the § 512(c) safe harbor because they were aware of apparent infringing activity due to the illicit website names.¹⁰⁹ The court held that “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.”¹¹⁰ A year later in *Io Group*, the District Court for the Northern District of California, cited *Perfect 10* and reiterated that describing photographs as illegal or stolen does not place the burden on a service provider to determine whether the photographs are illegal.¹¹¹ Recently, in *UMG Recordings*, the District Court for the Central District of California interpreted *Perfect 10* as concluding that website names such as “illegal.net” and “stolencelebritypics.com” are not red flags because they “did not signal apparent infringement.”¹¹² These three cases are overtly inconsistent with Congress’s decree that pirate directories that use slang terms in their URL are “obviously infringing.”¹¹³

The court in *Perfect 10* explained that the words “illegal” and “stolen” are not red flags because there might be other purposes for a website to use such names.¹¹⁴ The court speculated reasons for why the OSPs’ users described the sites as

¹⁰⁴ *Id.* (citing DMCA H. REP., *supra* note 7, at 7).

¹⁰⁵ *Perfect 10*, 488 F.3d at 1114. See also DMCA H. REP., *supra* note 7, at 58; DMCA S. REP., *supra* note 2, at 48.

¹⁰⁶ “Once a service provider is aware of a site containing such ‘red flags,’ the service provider would have apparent knowledge of the infringing activity.” *Corbis*, 351 F. Supp. 2d at 1108.

¹⁰⁷ *Perfect 10*, 488 F.3d at 1114.

¹⁰⁸ See DMCA H. REP., *supra* note 7, at 58; DMCA S. REP., *supra* note 2, at 48.

¹⁰⁹ *Perfect 10*, 488 F.3d at 1114.

¹¹⁰ *Id.*

¹¹¹ *Io Group*, 586 F. Supp. 2d at 1149 (citing *Perfect 10*, 488 F.3d at 1114).

¹¹² *UMG Recordings*, 665 F. Supp. 2d at 1108 (citing *Perfect 10*, 488 F.3d at 1114).

¹¹³ DMCA H. REP., *supra* note 7, at 58; DMCA S. REP., *supra* note 2, at 48.

¹¹⁴ *Perfect 10*, 488 F.3d at 1114.

such. This reasoning would apply to any alleged red flag and allow many OSPs to escape financial liability. For instance, the court applied this same reasoning to password-hacking websites when it held that these websites are not red flags because passwords may have been provided for promotional purposes or to collect subscribers' information.¹¹⁵ The same reasoning can equally apply to a user's disclaimer declaring that its pictures are stolen because the OSP would never truly know if the pictures are in fact stolen or if the disclaimer was used to simply attract viewers.

Another major flaw of the court's reasoning in *Perfect 10* is that the user's motive in its choice of website names is irrelevant. Congress instructed courts to apply the two parts of the red flag test to determine whether the OSP was aware of circumstances (the illicit website names), and if so, whether these circumstances, regardless of the motive behind their selection, were such that infringement is apparent. In the end, what truly matters is whether these words raise a red flag from which OSPs should not turn a blind eye. These cases, *Perfect 10*, *UMG Recordings*, and *Io Group*, show that "it can be almost impossible . . . to prove that any given moniker truly gives rise to enough knowledge indicating infringement to constitute a red flag."¹¹⁶

3. Password-Hacking Websites

In *Perfect 10*, defendant CWIE also hosted password-hacking websites.¹¹⁷ Password-hacking websites are websites that unlawfully provide users with log-in names and passwords to access other websites.¹¹⁸ *Perfect 10* argued that password-hacking websites obviously infringe, and therefore, constitute red flags. According to the court,

[P]roviding passwords that enable users to illegally access websites with copyrighted content may well amount to contributory infringement . . . [but] in 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.¹¹⁹

The court explained that the website may have been a

¹¹⁵ *Id.*

¹¹⁶ NIMMER & NIMMER, *supra* note 35, § 12B-05[B][1].

¹¹⁷ *Perfect 10*, 488 F.3d at 1114.

¹¹⁸ Opening Brief of Plaintiff-Appellant at 8 n.6, *Perfect 10, Inc. v. CCBill LLC*, *supra* note 92.

¹¹⁹ *Perfect 10*, 488 F.3d at 1114 (citing *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1012 n.2 (9th Cir. 2001)).

“hoax” or “out of date,”¹²⁰ or may have been provided as “a short-term promotion,” “to collect information from unsuspecting users,” or “to help users maintain anonymity without infringing.”¹²¹ Therefore, the court concluded that password-hacking websites, even though they provide users with illegal access to websites with copyrighted material, which may amount to contributory infringement, are not “*per se* ‘red flags’ of infringement.”¹²²

The court held that the defendant had no knowledge of the infringement despite the fact that Mr. Fisher, the designated agent¹²³ and the Executive Vice President of CCBill and CWIE, “openly admitted that such websites engaged in theft.”¹²⁴ This allegation was based on an email that Mr. Fisher wrote to a webmaster stating he was aware that the website “is allowing password trading . . . [which] constitutes ‘theft of services.’”¹²⁵ Mr. Fisher’s email clearly showed that the OSP was aware of circumstances (illegally providing passwords to carry out theft of services) from which infringement was apparent. The jury could have inferred that infringement is apparent to a reasonable person under the same circumstances, that is, to someone who bears the title of executive vice president and knows that the website it hosts engages in theft of services.

4. Federal Labeling Law Violation

As mentioned in Part III.A., the plaintiff in *Io Group* argued that Veoh’s user’s violation of the federal labeling law 18 U.S.C. § 2257¹²⁶ is a red flag of obvious infringement.¹²⁷ Plaintiff *Io Group* contended that from the violation one may infer “that the uploading user did not have authority to submit the content in question,” and therefore, that the user was not the legitimate producer of the sexually explicit material.¹²⁸ The court found that there was evidence in the record to show that Veoh was aware of the federal law¹²⁹ and “a fact question as to whether Veoh was aware that federal labeling laws might have

¹²⁰ *Perfect 10*, 488 F.3d at 1114.

¹²¹ *Id.*

¹²² *Id.*

¹²³ *Id.* at 1108.

¹²⁴ Opening Brief of Plaintiff-Appellant at 8, *Perfect 10, Inc. v. CCBill LLC*, *supra* note 92.

¹²⁵ *Id.*

¹²⁶ 18 U.S.C. § 2257(a) & (f) require producers of sexually explicit material to maintain certain records as to the performers depicted and to label each such work with a statement indicating where those records are located. 18 U.S.C. § 2257(a) & (f).

¹²⁷ *Io Group*, 586 F. Supp. 2d at 1149.

¹²⁸ *Id.*

¹²⁹ *Id.*

been violated.”¹³⁰ Notwithstanding these facts, the court still held that the absence of required labels, which was a federal law violation possibly indicating that the user was not the legitimate producer, “does not give rise to a genuine issue of material fact as to whether Veoh had the requisite level of knowledge or awareness” of the infringement.¹³¹ It is difficult to understand why the defendant is qualified for the DMCA safe harbor if the OSP must lack awareness of circumstances from which the infringing activity is apparent. If the OSP might have been aware of the circumstance (that a user violated a federal law), then the only way for the OSP to qualify for a safe harbor is to find that infringement was not apparent from the circumstance. Thus, although the federal labeling law violation suggests that there could be some infringing activity taking place, the court seems to conclude that a violation of the federal labeling law is not a red flag; and therefore, even if Veoh were aware of the violation, it was irrelevant to the red flag test.

5. Nature of Subject Matter and Professional Production

Io Group also alleged that the OSP’s user’s infringement was obvious because the works in question were of sexually explicit nature and were professionally created.¹³² The court held that the sexually explicit and professionally created nature of the works did not constitute per se red flags to impute knowledge or awareness to the OSP.¹³³ The court reasoned that today, there is little distinction between professional and amateur productions due to the video equipment available to the general public.¹³⁴ Io Group also claimed that the profile of one of the users who uploaded the work indicated that he was only seventeen years old, and therefore, not allowed to upload such works.¹³⁵ However, this fact was not considered in the red flag analysis because Io Group did not raise this argument when opposing Veoh’s motion as to the DMCA safe harbor.¹³⁶ The court found that the red flag test was not satisfied despite the defendant’s awareness of the sexually explicit and professional nature of the video clips and the possibility of the defendant’s awareness of the violation of federal labeling law

¹³⁰ *Id.*

¹³¹ *Id.*

¹³² *Id.*

¹³³ *Io Group*, 586 F. Supp. 2d at 1149.

¹³⁴ *Id.*

¹³⁵ *Id.* at 1149 n.10.

¹³⁶ *Id.* at 1149.

from which a reasonable person may infer that the uploading user was not the authorized producer of the videos.

6. General Awareness of Infringement

In *UMG Recordings* the court held that the OSP's general awareness of infringement, without more, is not enough to preclude application of the § 512(c) safe harbor.¹³⁷ The plaintiffs, members of UMG Recordings, Inc., brought a copyright infringement suit against Veoh Networks, Inc., an Internet video-sharing website.¹³⁸ In this case, the court discussed whether Veoh, an OSP, meets the § 512(c) safe harbor requirements.¹³⁹ The court granted Veoh's motion for summary judgment and found that Veoh was entitled to the DMCA § 512(c) safe harbor because (1) it expeditiously removed the infringing material when it acquired knowledge through the DMCA notices,¹⁴⁰ and (2) it had no actual or apparent knowledge of the infringing files that it did not remove.¹⁴¹

Plaintiffs argued that Veoh had apparent knowledge because its founders, employees, and investors knew that "widespread infringement was occurring on the Veoh system."¹⁴² However, the court held that even if this were true, general awareness of infringement, *without more*, is not enough to raise a red flag.¹⁴³ The court concluded that Veoh was not aware of red flags, "notwithstanding its knowledge of the general proposition that infringing material is often uploaded to websites."¹⁴⁴ However, the court does not explain what *more* is needed in addition to general awareness of infringement. The only guidance the court provides is that it followed the principle that the burden is on the copyright holder to provide notice of the infringement, and that "it takes willful ignorance of readily apparent infringement to find a 'red flag.'"¹⁴⁵

IV. WHY DO COURTS SEEM RELUCTANT TO FIND APPARENT KNOWLEDGE THROUGH THE RED FLAG TEST?

The fact that no court has found apparent knowledge through the red flag test suggests judicial reluctance to do so. There are three possible reasons why courts are rendering the

¹³⁷ *UMG Recordings*, 665 F. Supp. 2d at 1111.

¹³⁸ *Id.* at 1100.

¹³⁹ *Id.* at 1108-12.

¹⁴⁰ *Id.*

¹⁴¹ *Id.* at 1108.

¹⁴² *Id.* at 1111.

¹⁴³ *UMG Recordings*, 665 F. Supp. 2d at 1111 (emphasis added).

¹⁴⁴ *Id.* at 1112.

¹⁴⁵ *Id.* at 1108.

red flag test essentially unattainable: first, 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. However, these reasons do not justify the currently insurmountable standard of the red flag test. In fact, a standard that allows a copyright holder to establish apparent knowledge through the red flag test is necessary to achieve the DMCA's purpose in encouraging copyright holders and OSPs to cooperate in detecting and dealing with infringement.

A. *To Promote Internet Development, Free Flow of Information, and Electronic Commerce*

The DMCA was “designed to facilitate the robust development and worldwide expansion of electronic commerce, communications, research, development, and education.”¹⁴⁶ OSPs play a key role in promoting Internet development and electronic commerce as it allows millions of people to access the World Wide Web. The DMCA's safe harbors help eligible OSPs maintain a viable business by protecting them from liability due to third party copyright infringement.

1. To Relieve OSPs of the Burden to Investigate

To advance Internet development, the DMCA placed the burden to investigate and monitor potential infringement on the copyright holder.¹⁴⁷ Congress did not mandate an OSP to “monitor its service or affirmatively seek facts indicating infringing activity” in order to qualify for the safe harbors under § 512.¹⁴⁸ The court in *Perfect 10* claimed to honor this legislative intent when it held that describing photographs as illegal or stolen was not a red flag because the OSP does not have the burden to investigate whether infringement is actually occurring on its site.¹⁴⁹ However, there was no burden to investigate whether the photographs were in fact illegal because infringement was obvious since the photographs were described as illegal. The photos were uploaded to websites named “illegal.net” and “stolencelebritypics.com.” If describing photographs as illegal is not enough to raise a red flag, then it is difficult to understand what is. Congress clearly stated that

¹⁴⁶ DMCA S. REP., *supra* note 2, at 1-2.

¹⁴⁷ *Id.*

¹⁴⁸ DMCA H. REP., *supra* note 7, at 53; DMCA S. REP., *supra* note 2, at 44. See also *Hendrickson*, 298 F. Supp. 2d at 916.

¹⁴⁹ *Perfect 10*, 488 F.3d at 1114.

although an OSP has no obligation to investigate copyright infringement, it cannot avail itself of the safe harbor if it turned a blind eye on red flags of obvious infringement.¹⁵⁰ Congress intended to encourage the OSP and the copyright holder to cooperate in detecting infringement,¹⁵¹ rather than to allow the OSP to contribute to infringement by providing services to infringers.

2. To Provide Certainty to OSPs

To provide OSPs with the highest level of certainty, one simple solution would be to completely read out the red flag provision so that the OSP is never imputed with knowledge when it lacks actual knowledge. However, until the Legislature decrees otherwise, one must keep in mind Congress's purpose to promote both Internet development and electronic commerce. Infringement on the Internet may stand in the way of electronic commerce since copyright holders who sell its products on the Internet will not be able to maximize profits when there are thousands of pirate copies circulating through the Internet. If copyright holders decide not to use the Internet as a medium of commerce, then this might impact both Internet development and electronic commerce. Hence, it is necessary to balance the need for certainty and for minimizing infringement with the red flag test, as Congress contemplated. Without the red flag test, an OSP who chooses to ignore a red flag will be free of liability, since actual knowledge is difficult to prove, and will continue to provide services to the infringing user.

One may argue that an OSP would not be free of liability even without the red flag test because there are other means available to hold the OSP liable, such as stripping the OSP of the safe harbor by finding failure to implement a termination policy¹⁵² or receipt of direct financial benefit from the infringing activity.¹⁵³ However, although there are other grounds to disqualify the OSP of the safe harbor, the red flag test must remain accessible because it serves an important purpose: it encourages OSPs to assist in detection of infringement, rather than to wait for a notification while infringement occurs.

¹⁵⁰ DMCA H. REP., *supra* note 7, at 57; DMCA S. REP., *supra* note 2, at 48.

¹⁵¹ DMCA H. REP., *supra* note 7, at 49.

¹⁵² In *Perfect 10 v. Cybernet*, the court found that Cybernet cannot avail itself of the § 512 safe harbors because there is a strong likelihood that Cybernet cannot establish that it has reasonably implemented a policy directed at terminating repeat infringers. 213 F. Supp. 2d 1146, 1183 (C.D. Cal. 2002).

¹⁵³ 17 U.S.C. § 512(c).

B. *To Place the Burden on the Most Efficient Cost Bearer*

Another reason why courts are reluctant to find apparent knowledge through the red flag test is because copyright holders are in the most efficient position to bear the costs of investigating infringement.

In most cases, copyrighted works have both authorized and unauthorized copies in the marketplace, making it extremely difficult and expensive for OSPs to distinguish these two groups. While the OSP would need to incur expenses to determine whether the users' activity is in fact infringement, a copyright holder would know whether she authorized the copy or distribution. However, there are two steps in terminating copyright infringement. First, suspicious activity must be detected or brought to the OSP's attention. Second, someone must determine whether there is actual infringement. It can hardly be contested that the copyright owner is in a better position to carry out the second step, which is to determine whether there is actual infringement, once suspicious activity is detected. However, whether the copyright owner is in a better position to detect suspicious activity or infringing users is debatable. To uncover infringement, one would need to search through the OSP's users' listings or be notified by viewers. Although both the copyright holder and the OSP would need to search the listings, the OSP is in a better position to learn of the potential infringement because a viewer who comes across infringement on a website might find it more convenient to report it to the website rather than to locate the copyright holder. Under § 512(i), the OSP should already have a reasonably implemented termination policy to deal with infringement on its site, and therefore, should have better eyes and ears to capture suspicious activity. In many instances, the OSP also reserves the right and absolute discretion on the subscription agreement to "remove, screen, or edit any content" that commits infringement.¹⁵⁴

If the OSP is in a better position to detect suspicious activity while the copyright owner is in a better position to determine whether there is actual infringement, then the red flag test is an appropriate tool to encourage copyright holders and OSPs to cooperate in detecting and dealing with copyright infringement. An OSP that learns of circumstances of *apparent* infringement must act expeditiously to remove or disable ac-

¹⁵⁴ *Corbis*, 351 F. Supp. 2d at 1095.

cess to the potentially infringing material.¹⁵⁵ A copyright holder, who learns of actual infringement, should properly notify the OSP. The OSP loses the safe harbor if it acquires actual knowledge of infringement or awareness of circumstances from which infringement is apparent, and fails to remove it. Thus, under the red flag test, the burden to determine whether there is actual infringement would remain with the copyright holder, while OSPs would not be able to turn “a blind eye to ‘red flags’ of obvious infringement.”¹⁵⁶

C. *To Avoid Higher Costs to Consumers*

The existence of a red flag test generates costs to the consumer. If apparent knowledge may be found through the red flag test, OSPs would be compelled to monitor its services. These expenses will be passed down onto the OSPs’ users who will then pass them down to consumers. Courts may want to prevent these costs by making it practically impossible to find apparent knowledge through the red flag test and eventually obliterating its existence.

However, if the red flag test is nonexistent, then the costs to consumers might be even higher. First, infringement on the Internet will go undetected and copyright holders may decide to raise their prices to account for lost profit. For instance, while a song may be sold for ninety-nine cents on the Internet for a limited use, a copyright owner might decide to charge more because use will no longer be limited due to infringement. Second, copyright holders will probably be more aggressive at screening websites incurring costs that will be passed on to consumers as well. If it is impossible for the copyright owner to establish apparent knowledge through the red flag test, then the copyright owner will have to monitor websites, determine whether there is actual infringement, and send proper notification to disqualify the OSP from safe harbor status. In the end, such system of monitoring and sending proper notification even where infringement is obvious will create additional costs to customers.

¹⁵⁵ 17 U.S.C. § 512(c)(1)(A) (emphasis added).

¹⁵⁶ Under the red flag test 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.” DMCA H. REP., *supra* note 7, at 57.

V. AN INSURMOUNTABLE STANDARD FOR FINDING APPARENT KNOWLEDGE

A. *Implications of an Insurmountable Standard*

To constitute a red flag under the DMCA “the ‘flag’ must be brightly red indeed—and be waving blatantly in the provider’s face . . . [but] it appears that not even blood crimson is enough.”¹⁵⁷ Such an insurmountable standard for the red flag test provides no incentive for OSPs to cooperate with copyright holders to detect and deal with potential infringement because OSPs are certain that apparent knowledge will not be imputed on them absent a statutory compliant notice.

OSP s could cooperate with copyright holders in dealing with copyright infringement by taking down infringing material and monitoring the services they provide to its users. However, Congress does not mandate OSPs to monitor, and courts have discouraged OSPs from doing so by setting an insurmountable red flag standard. Case law discussing the red flag test indicates that it is easy for an OSP to allege no knowledge to escape monetary liability. Without the red flag test, the OSP has no knowledge under the DMCA § 512(c) safe harbor unless the OSP receives proper notice or the copyright owner proves that the OSP has actual knowledge of infringement.

Since the standard to find apparent knowledge through the red flag test is practically unattainable, OSPs have no reason or incentive to monitor or to take action even if it has suspicion or is almost certain that infringement is taking place. In fact, an OSP that chooses to monitor runs the risk of acquiring actual knowledge (for instance, by discovering a disclaimer in which the user admits to infringement), and the OSP may no longer claim lack of knowledge. If it is impossible for a plaintiff to establish a red flag, then an OSP that does not receive proper notification will always take its chances, have no incentive to cooperate with the copyright owner, let the copyright owner sue, and claim immunity under the safe harbor to dismiss the case.

B. *An Accessible Standard is Necessary to Achieve Congressional Intent*

Judicial application of the red flag test has been inconsistent with legislative intent because courts have made it practi-

¹⁵⁷ NIMMER & NIMMER, *supra* note 35, § 12B-04[A][1].

cally impossible to establish apparent knowledge under the red flag test. However, until the Legislature decides otherwise, the red flag test exists and should be used to impute OSPs with apparent knowledge when they are “aware of facts or circumstances from which infringing activity is apparent.”¹⁵⁸ An accessible standard is necessary to balance the interests of copyright holders and OSPs and to encourage them to cooperate in detecting and dealing with infringement.

An accessible standard would require courts to find apparent knowledge under the red flag test where the OSP is aware of circumstances in which infringement is apparent from a “brief and casual viewing,”¹⁵⁹ as contemplated by Congress. Under this standard, pirate directories that “use words such as ‘pirate,’ ‘bootleg,’ or slang terms in their URL . . . to make their illegal purpose obvious”¹⁶⁰ would constitute red flags, and an OSP that views such directory would not qualify for the § 512(c) safe harbor. As Congress explained, “safe harbor status for a provider that views such a site and then establishes a link to it would not be appropriate” because the “infringing nature of such sites would be apparent from even *a brief and casual viewing*.”¹⁶¹ This brief and casual viewing standard complies with legislative intent because it does not require OSPs to constantly monitor and hunt for potential infringement. Instead, where an OSP is aware of circumstances in which infringement is apparent to a reasonable person from a brief and casual viewing, it would need to take prompt action to remove or disable access to the infringing material.¹⁶²

Applying an accessible standard in *Perfect 10*, the defendants would not have qualified for the § 512(c) safe harbor because the website names “illegal.net” and “stolencelebritypics.com” cry infringement. In addition, the fact that the OSPs’ executive vice president was aware that the password-hacking websites were engaged in theft of services should have been enough to deny the OSPs any safe harbor status. In *Io Group* the OSP’s motion for summary judgment arguing that it qualified for the safe harbor under § 512(c) should have been denied. The court should have held that a violation of a federal labeling law on sexually explicit materials, from which a reasonable person may infer that the uploading user was not

¹⁵⁸ 17 U.S.C. § 512(c)(1)(A)(ii).

¹⁵⁹ DMCA H. REP., *supra* note 7, at 58; DMCA S. REP., *supra* note 2, at 48.

¹⁶⁰ DMCA H. REP., *supra* note 7, at 58; DMCA S. REP., *supra* note 2, at 48.

¹⁶¹ DMCA H. REP., *supra* note 7, at 58 (emphasis added); DMCA S. REP., *supra* note 2, at 48.

¹⁶² 17 U.S.C. § 512(c)(1)(A)(iii).

an authorized producer, is a red flag, and the court should have allowed the case to move forward to determine whether the OSP in fact knew of this violation.

If the red flag test is accessible to copyright holders, in that they may be able to establish apparent knowledge where infringement is objectively apparent even though they did not notify the OSP, then OSPs would be encouraged to cooperate with copyright holders to detect infringement. Copyright holders who know of actual infringement would notify the OSP, and OSPs that are aware of facts from which infringement is objectively apparent from a brief and casual viewing would have an incentive to take action. Since there is a chance that the suspicious circumstance is one from which infringement is apparent, OSPs that learn of suspicious activity would take action to monitor, investigate, or remove the apparent infringing activity because they may be imputed with apparent knowledge.

Congress stated that “a service provider need not monitor its service or affirmatively seek facts indicating infringing activity.”¹⁶³ Congress further explained that it did not intend to undermine the knowledge standard of § 512(c) by “suggesting that a provider must investigate possible infringements, monitor its service, or make difficult judgments as to whether conduct is or is not infringing.”¹⁶⁴ However, an accessible standard will not overburden OSPs with a duty to investigate because the OSP only needs to take action when infringement is clearly apparent from the surrounding circumstances. This achieves the dual goal of not imposing the OSP with an onerous task, and at the same time, promoting cooperation between the OSP and the copyright holder.

Moreover, this standard does not undermine Congress’s intent to provide OSPs with greater certainty concerning their liability due to users’ infringement because apparent knowledge would only be found if the circumstances clearly point to apparent infringement. A high, but not impossible, standard to satisfy the red flag test provides certainty to OSPs regarding their legal exposure for third party infringement, and at the same time deters OSPs from turning a blind eye on apparent infringement.

¹⁶³ DMCA H. REP., *supra* note 7, at 53; DMCA S. REP., *supra* note 2, at 44.

¹⁶⁴ DMCA H. REP., *supra* note 7, at 61.

CONCLUSION

The DMCA was created with the purpose of facilitating the development of electronic commerce and communications in the digital age by encouraging OSPs and copyright holders to cooperate in detecting copyright infringement. However, courts' decisions in recent cases have been inconsistent with this purpose. While courts have managed to read out the red flag test provision by finding it unsatisfied time after time, the DMCA's purpose is better achieved with a more accessible standard. Such a standard allows copyright holders to establish apparent knowledge where the OSP is aware of circumstances from which infringement is apparent from a brief and casual viewing. In addition, an accessible standard encourages parties to work together and continues to provide OSPs certainty regarding their legal exposure.

*Liliana Chang**

* Articles Editor, *Cardozo Arts & Ent. L.J.* (2009-2010), J.D. Candidate, Benjamin N. Cardozo School of Law (2010); B.B.A., summa cum laude, Finance & Investments, Macaulay Honors College at Baruch College (2005). I would like to give special thanks to my parents, siblings, brother-in-law, and Victor Law for their love and everlasting support. Also, I would like to thank Debra Weinstein, Professor Stewart E. Sterk, and the 2009-2010 AELJ editorial staff for their guidance in writing this Note. © 2010 Liliana Chang.