

**An Overview of the Digital Millennium Copyright Act (DMCA)  
“Safe Harbors” for Online Service Providers (OSPs)  
(17 U.S.C. § 512<sup>1</sup>)**

**I. What are the DMCA’s OSP safe harbors?**

**A. The “safe harbors” are limitations on liability, not copyright exceptions.**

1. “The [safe harbor] limitations ... protect qualifying service providers from liability for **all monetary relief** for direct, vicarious and contributory infringement. Monetary relief is defined in subsection [(k)(2)] as encompassing damages, costs, attorneys’ fees, and any other form of monetary payment. These subsections **also limit injunctive relief** against qualifying service providers to the extent specified in subsection [(j)].” (Senate Report, p.40<sup>2</sup>).
2. Injunctive relief is limited to the following for conduct falling within the 512(a) “conduit” safe harbor (17 U.S.C. § 512(j)(1)(B)):
  - a) “An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is using the provider's service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.”
  - b) “An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States.”
3. Injunctive relief is limited to the following for conduct falling within the 512(b), (c) or (d) safe harbors (17 U.S.C. § 512(j)(1)(A)):
  - a) “An order restraining the service provider from providing access to infringing material or activity residing at a particular online site on the provider's system or network.”
  - b) “An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.”
  - c) “Such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified

---

<sup>1</sup> The complete statutory text can be found at the Copyright Office website:  
<<http://www.copyright.gov/title17/92chap5.html#512>>.

<sup>2</sup> The complete legislative history of the DMCA, including the Senate Judiciary Committee Report, S. Rep. 105-190, can be found at the Home Recording Rights Coalition website:  
<[http://www.hrrc.org/dmca/dmca\\_history.html](http://www.hrrc.org/dmca/dmca_history.html)>.

in the order of the court at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose.”

**B. Falling outside the safe harbors does not make you liable for infringement.**

1. “The failure of a service provider's conduct to qualify for limitation of liability under this section shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title or any other defense.” (17 U.S.C. § 512(I)).
2. “New section 512 does not define what is actionable copyright infringement in the online environment, and does not create any new exceptions to the exclusive rights under copyright law. ... Even if a service provider’s activities fall outside the limitations on liability specified in the bill, the service provider is not necessarily an infringer; liability in these circumstances would be adjudicated based on the doctrines of direct, vicarious or contributory liability for infringement as they are articulated in the Copyright Act and in the court decisions interpreting and applying that statute, which are unchanged by section 512. In the event that a service provider does not qualify for the limitation on liability, it still may claim all of the defenses available to it under current law.” (Senate Report, p.55).
3. *See Perfect 10 v. CCBill*, 488 F.3d 1102, 1109 (9th Cir. 2007) (“These safe harbors limit liability but ‘do not affect the question of ultimate liability under the various doctrines of direct, vicarious, and contributory liability.’”); *Io Group v. Veoh Networks*, \_\_\_ F.Supp.2d \_\_\_, 2008 WL 4065872 at \*7 (N.D. Cal. Aug. 27, 2008) (same); *Perfect 10 v. Cybernet Ventures*, 213 F.Supp.2d 1146, 1174 (C.D. Cal. 2002) (same).
4. **So compliance with the requirements of the safe harbors is optional for service providers, not mandatory.** The increased certainty provided by the safe harbors, however, creates a strong incentive for service providers to take advantage of them, if they can.

**C. The DMCA safe harbors only apply to copyright infringement (not trademark or patent infringement, or other causes of action).**

1. Most service providers, however, also enjoy broad immunity from most state law causes of action, thanks to Section 230 of the Communications Decency Act (“CDA 230”). *See, e.g., Perfect 10 v. CCBill*, 488 F.3d 1102, 1118-19 (9th Cir. 2007) (CDA 230 preempts all state intellectual property statutes, including right of publicity); *Barrett v. Rosenthal*, 146 P.3d 510, 51 Cal.Rptr.3d 55 (Cal. 2006).

**D. The safe harbors only apply to “service providers” performing certain “functions” (defined in § 512(a), (b), (c) and (d)).**

1. “To qualify for these protections service providers must meet the conditions set forth in subsection [(i)], and service providers’ activities at

issue must involve a function described in subsection (a), (b), (c), (d) or [(g)], respectively.” (Senate Report, p.41)

2. So copyright owners have an incentive to characterize their lawsuits as involving activities that fall outside the defined functions protected by the safe harbors (e.g., intermediate copying, trans-coding, server-side data processing).

## II. Who is a “service provider”?

### A. Safe harbors only cover “service providers”

### B. Two definitions of “service provider”

1. In order to qualify for the 512(a) “conduit” safe harbor, you must satisfy the narrow definition of “service provider.” In order to qualify for the 512(b), (c) or (d) safe harbors, in contrast, you need only satisfy the broad definition.
2. *Narrow definition for “conduit” safe harbor:* “As used in [section 512](a), the term "service provider" means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.” (17 U.S.C. § 512(k)(1)(A).)
  - a) E.g., traditional ISPs, like Verizon or Comcast, providing simple bandwidth.
  - b) There has been some uncertainty regarding the outer limits of the narrower 512(a) definition, especially as applied to P2P systems where end-users do the transmitting, routing, or provision of connections, rather than the OSP. *Compare Perfect 10 v. CCBill*, 488 F.3d 1102, 1116 (9th Cir. 2007) (“We reject Perfect 10’s argument that CCBill is not eligible for immunity under § 512(a) because it does not itself transmit the infringing material.... There is no requirement in the statute that the communications must themselves be infringing....”) *with A&M Records v. Napster*, 2000 WL 573136 (N.D. Cal. 2000) (“Napster enables or facilitates the initiation of connections, but these connections do not pass through the system within the meaning of § 512(a).”).
3. *Broad definition other safe harbors:* “As used in this section, other than [section 512](a), the term "service provider" means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph [512(k)(1)](A).” (17 U.S.C. § 512(k)(1)(B).)
  - a) Courts have held that Amazon, eBay, and Aimster all qualify as “service providers” under this definition. *See Corbis v. Amazon.com*, 351 F.Supp.2d 1090 (W.D. Wash. 2004) (Amazon);

334 F.3d 643, 655 (7th Cir. 2003) (Aimster); *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1087 (C.D. Cal. 2001) (eBay).

- b) In the words of one court: “A plain reading of [17 U.S.C. § 512(k)] reveals that ‘service provider’ is defined so broadly that we have trouble imagining the existence of an online service that would not fall under the definitions....” *In re Aimster Copyright Litig.*, 252 F.Supp.2d 634, 658 (N.D. Ill. 2002), *aff’d*, 334 F.3d 643 (7th Cir. 2003).

### III. What “functions” are covered?

#### A. 512(a): “conduit” or ISP safe harbor

1. “A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if (1) the transmission of the material was initiated by or at the direction of a person other than the service provider; (2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider; (3) the service provider does not select the recipients of the material except as an automatic response to the request of another person; (4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and (5) the material is transmitted through the system or network without modification of its content.” (17 U.S.C. § 512(a))
2. “Subsections (a)(1) through (5) limit the range of activities that qualify under this subsection to ones in which a service provider plays the role of a ‘conduit’ for the communications of others.” (Senate Report, p. 41); *See Perfect 10 v. CCBill*, 488 F.3d 1102, 1116 (9th Cir. 2007) (“Section 512(a) provides a broad grant of immunity to service providers whose connection with the material is transient.”).
3. This is the most expansive safe harbor for a service provider, as it has the fewest prerequisites and disqualifiers, but is only available to those who can meet the narrow definition of “service provider” and only covers “conduit” activities that fall within the statutory language. *See, e.g., Ellison v. Robertson*, 357 F.3d 1072 (9th Cir. 2004) (holding that AOL’s provision of Usenet newsgroups to subscribers falls within 512(a)).

**B. 512(b): caching**

1. “For subsection (b) to apply, the material must be made available on an originating site, transmitted at the direction of another person through the system or network operated by or for the service provider to a different person, and stored through an automatic technical process so that users of the system or network who subsequently request access to the material from the originating site may obtain access to the material from the system or network. Subsections (b)(1) through (b)(5) further refine the circumstances under which subsection (b) applies....” (Senate Report, p. 42).
2. “In terminology describing current technology, this storage is a form of “caching,” which is used on some networks to increase network performance and to reduce network congestion generally, as well as to reduce congestion and delays to popular sites. This storage is intermediate in the sense that the service provider serves as an intermediary between the originating site and ultimate user. The material in question is stored on the service provider’s system or network for some period of time to facilitate access by users subsequent to the one who previously sought access to it.” (Senate Report, p. 42).
3. There is very little case law on the 512(b) safe harbor, and it is not clear that the statutory language adequately addresses the sophisticated caching activities that have arisen since 1998. However, one court has held that Google’s Web cache is covered by 512(b). *See Field v. Google*, 412 F.Supp.2d 1106 (D. Nev. 2006).

**C. 512(c): hosting**

1. Safe harbor applies for any “infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider...” (17 U.S.C. § 512(c)).
2. “Examples of such storage include providing server space for a user’s web site, for a chatroom, or other forum in which material may be posted at the direction of users.” (Senate Report, p. 44).
3. Requires designation and registration of a “copyright agent” and implementation of a “notice-and-takedown” regime. (see below).
4. Subject to two disqualifiers: “actual or red flag knowledge” and “control + direct financial benefit” (see below).
5. Numerous activities beyond “providing server space for a user’s web site, for a chatroom, or other forum” have been found to fall within the 512(c) safe harbor. *See, e.g., Io Group v. Veoh Networks*, \_\_\_ F.Supp.2d \_\_\_, 2008 WL 4065872 (N.D. Cal. Aug. 27, 2008) (video hosting); *Corbis v. Amazon*, 351 F. Supp. 2d 1090 (W.D. Wash. 2004) (Amazon zShops); *CoStar v. LoopNet*, 164 F. Supp. 2d 688 (D. Md. 2001), *aff’d*, 373 F.3d

544 (4th Cir. 2004) (user-generated real estate listings); *Hendrickson v. eBay*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001) (eBay listings).

**D. 512(d): information location tools (linking and search engines)**

1. Safe harbor applies for any “infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link....” (17 U.S.C. § 512(d)).
2. “The reference to ‘infringing activity’ is intended to refer to wrongful activity that is occurring at the location to which the link or reference refers, without regard to whether copyright infringement is technically deemed to occur at that location or at the location where the material is received. The term information location tools includes, for example: a directory or index of online sites or material such as a search engine that identifies pages by specified criteria, a reference to other online material such as a list of recommended sites, a pointer that stands for an Internet location or address, or a hypertext link which allows users to access material without entering its address.” (Senate Report, p.47).
3. Requires designation and registration of a “copyright agent” and implementation of a “notice-and-takedown” regime. (see below).
4. Subject to two disqualifiers: “actual or red flag knowledge” and “control + direct financial benefit” (see below).

**IV. Prerequisites and Disqualifiers**

**A. Prerequisites applicable to all safe harbors (512(i))**

1. Policy of Terminating Repeat Infringers
  - a) Service provider must “adopt and reasonably implement, and inform subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers.” (17 U.S.C. § 512(i)(1)(A)).
  - b) The statute provides no definition of “repeat infringer”—can mere allegations or DMCA takedown notices make someone a “repeat infringer”? *Compare* Nimmer & Nimmer, 3 NIMMER ON COPYRIGHT § 12B.10[B][3](describing what makes a “repeat infringer” and concluding that allegations or multiple takedown notices alone are insufficient); *Corbis v. Amazon*, 351 F.Supp.2d at 1105 n.9 (“[N]otices alone do not ... conclusively determine that the user is an infringer.”), *with Perfect 10 v. CCBill*, 340 F.Supp.2d 1077, 1088 (C.D. Cal. 2004) (multiple 512(c) takedown notices requires termination of the user under 512(i)), *aff'd on other grounds*, 488 F.3d 1102 (9th Cir. 2007).

- c) “[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.” *Perfect 10 v. CCBill*, 488 F.3d 1102, 1109 (9th Cir. 2007); *see also Ellison v. Robertson*, 357 F.3d 1072, 1080 (9th Cir. 2004) (failing to read emails sent to registered Copyright Agent may not be reasonable implementation); *Io Group v. Veoh Networks*, \_\_\_ F.Supp.2d \_\_\_, 2008 WL 4065872 at \*8-10 (N.D. Cal. Aug. 27, 2008) (finding that infringer termination policies of video hosting service had been reasonably implemented); *Perfect 10 v. Cybernet Ventures*, 213 F. Supp. 2d 1146, 1176-78 (C.D. Cal. 2002) (finding little likelihood that defendant had adequately implemented a policy of terminating infringers).
- d) Courts have concluded that a policy is reasonably implemented where a service provider blocked terminated users from re-registering from the same email addresses, but did not also screen users by IP address or other means. *See Io Group v. Veoh Networks*, \_\_\_ F.Supp.2d \_\_\_, 2008 WL 4065872 at \*10 (N.D. Cal. Aug. 27, 2008) (“[S]ection 512(i) does not require service providers to track users in a particular way or to affirmatively police users for evidence of repeat infringement.”); *see also Corbis v. Amazon*, 351 F.Supp.2d at 1104 (“The mere fact that [the repeat infringer] appeared on zShops under a different user name and identity does not, by itself, create a legitimate question of fact regarding the procedural implementation of Amazon’s termination policy.”).

2. Accommodate Technical Measures

- a) Service provider must “accommodate and not interfere with standard technical measures...used by copyright owners to identify or protect copyrighted works.” (17 U.S.C. § 512(i)(1)(B))
- b) In order to qualify as a “standard technical measure,” the measure must have been developed “pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process,” be available on RAND terms, and not impose “substantial costs” on service providers.
- c) As of 2008, nothing appears to qualify as a “standard technical measure” under the definition of the statute, as no “broad consensus” has emerged from any relevant “multi-industry standards process.”

**B. Additional prerequisites for § 512(b), (c), and (d)**

- 1. Designate a Copyright Agent

- a) Service provider must designate an agent to receive copyright infringement notices, register the agent with the Copyright Office (\$80 filing fee), and make the agent's contact information available on its website. (17 U.S.C. § 512(c)(2); 37 CFR § 201.38).
- b) The Copyright Office makes the list of registered copyright agents available on its website at <<http://www.copyright.gov/onlinesp/>>.

2. Notice-and-Takedown

- a) Service provider must “upon notification of claimed infringement as described in paragraph [512(c)](3), respond[] expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.” (17 U.S.C. § 512(c)(1)(C)); *see Io Group v. Veoh Networks*, \_\_\_ F.Supp.2d \_\_\_, 2008 WL 4065872 at \*15 (N.D. Cal. Aug. 27, 2008) (finding no material issue of fact where service provider responded to takedown notices “on the same day the notice is received (or within a few days thereafter).”).
- b) In order to be effective, takedown notices must be in writing and: (1) contain the physical or electronic signature of claimant; (2) identify the work allegedly infringed; (3) identify the allegedly infringing material sufficiently to permit its removal or limit access; (4) provide information sufficient to contact the party providing the notice; (5) contain a statement that the complaining party has a good faith belief that use of the material is not authorized; and (6) contain a statement that the information in the notice is accurate and, under penalty of perjury, that either the owner or the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed. *See* 17 U.S.C. § 512(c)(3). *See also Perfect 10 v. CCBill*, 488 F.3d 1102, 1112 (9th Cir. 2007) (“The statute thus signals that substantial compliance means substantial compliance with *all* of § 512(c)(3)’s clauses, not just some of them.”); *but see ALS Scan v. RemarQ Communities*, 239 F.3d 619, 625 (4th Cir. 2001) (suggesting that substantial compliance is sufficient in some circumstances).
- c) “The DMCA notification procedures place the burden of policing copyright infringement—identifying the potentially infringing material and adequately documenting the infringement—squarely on the owners of the copyright.” *Perfect 10 v. CCBill*, 488 F.3d 1102, 1113 (9th Cir. 2007).
- d) *Counter-Notice and Putback*: Section 512(g) creates a “counter-notice” regime protecting service providers from liability both for taking down material in response to infringement notices, and for restoring access (“put-back”) to material upon receiving a “counter-notice” from a subscriber contesting the infringement notice. It is important to note, however, that a “counter-notice”



regime is not a pre-requisite for the DMCA safe harbor—instead, it provides a service provider with protection vis-à-vis its own subscribers.

**C. Disqualifiers (only for § 512(c) and (d))**

1. Actual or “Red Flag” Knowledge

- a) A service provider enjoys the (c) and (d) safe harbors only so long as it:

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

(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent [e.g., “red flag” knowledge]; or

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

17 U.S.C. § 512(c)(1)(A); § 512(d)(1).

- b) “Under this standard, a service provider would have no obligation to seek out copyright infringement, but it would not qualify for the safe harbor if it had turned a blind eye to ‘red flags’ of obvious infringement.” (Senate Report, p. 48).

- c) “For instance, the copyright owner could show that the provider was aware of facts from which infringing activity was apparent if the copyright owner could prove that the location was clearly, at the time the directory provider viewed it, a ‘pirate’ site of the type described below, where sound recordings, software, movies or books were available for unauthorized downloading, public performance or public display. Absent such ‘red flags’ or actual knowledge, a directory provider would not be similarly aware merely because it saw one or more well known photographs of a celebrity at a site devoted to that person. The provider could not be expected, during the course of its brief cataloguing visit, to determine whether the photograph was still protected by copyright or was in the public domain; if the photograph was still protected by copyright, whether the use was licensed; and if the use was not licensed, whether it was permitted under the fair use doctrine.” (Senate Report, p. 48).

- d) “The important intended objective of this standard is to exclude sophisticated ‘pirate’ directories—which refer Internet users to other selected Internet sites where pirate software, books, movies, and music can be downloaded or transmitted—from the safe harbor. Such pirate directories refer Internet users to sites that are obviously infringing because they typically use words such as

‘pirate,’ ‘bootleg,’ or slang terms in their uniform resource locator (URL) and header information to make their illegal purpose obvious to the pirate directories and other Internet users.” (Senate Report, p. 48); *but see Perfect 10 v. CCBill*, 488 F.3d 1102, 1114 (9th Cir. 2007) (“illegal.net” and “stolencelebritypics.com” do not constitute red flags, as describing material as “illegal” or “stolen” may be an attempt to increase appeal, rather than an admission; site featuring hacked passwords also insufficient to be red flag of infringement).

- e) “In this way, the ‘red flag’ test in section 512(d) strikes the right balance. The common-sense result of this ‘red flag’ test is that online editors and catalogers would not be required to make discriminating judgments about potential copyright infringement. If, however, an Internet site is obviously pirate, then seeing it may be all that is needed for the service provider to encounter a ‘red flag.’ A provider proceeding in the face of such a red flag must do so without the benefit of a safe harbor.” (Senate Report, p.49).
- f) “The knowledge or awareness standard should not be applied in a manner which would create a disincentive to the development of directories which involve human intervention. Absent actual knowledge, awareness of infringement as provided in subsection (d) should typically be imputed to a directory provider only with respect to pirate sites or in similarly obvious and conspicuous circumstances, and not simply because the provider viewed an infringing site during the course of assembling the directory.” (Senate Report, p. 49).
- g) Cases interpreting the “knowledge disqualifier” include *Perfect 10 v. CCBill*, 488 F.3d 1102, 1114 (9th Cir. 2007) (noncompliant notices do not count toward knowledge, use of “illegal” or “stolen” in domain name does not create red flag knowledge for hosting service); *Io Group v. Veoh Networks*, \_\_\_ F.Supp.2d \_\_\_, 2008 WL 4065872 at \*14 (N.D. Cal. Aug. 27, 2008) (“[A]pparent knowledge requires evidence that a service provider turned a blind eye to ‘red flags’ of obvious infringement.”); *Corbis v. Amazon*, 351 F. Supp. 2d 1090, 1108-09 (W.D. Wash. 2004) (neither general knowledge of infringement on the site nor third party notices are not enough to constitute a “red flag”); *Hendrickson v. Amazon*, 298 F. Supp. 2d 914, 917 (C.D. Cal. 2003) (Amazon lacked prospective knowledge of infringing DVD sales, even after rightsholder informed it that the title in question had never been released on DVD); *Hendrickson v. eBay*, 165 F. Supp. 2d 1082, 1093 (C.D. Cal. 2001).

## 2. Control + Direct Financial Benefit

- a) A service provider will be disqualified from the (c) and (d) safe harbors if it “receive[s] a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity.” (17 U.S.C. § 512(c)(1)(B); § 512(d)(2))
- b) “In determining whether the financial benefit criterion is satisfied, courts should take a common-sense, fact-based approach, not a formalistic one. In general, a service provider conducting a legitimate business would not be considered to receive a ‘financial benefit directly attributable to the infringing activity’ where the infringer makes the same kind of payment as non-infringing users of the provider’s service. Thus, receiving a one-time set-up fee and flat periodic payments for service from a person engaging in infringing activities would not constitute receiving a ‘financial benefit directly attributable to the infringing activity.’ Nor is subparagraph (B) intended to cover fees based on the length of the message (per number of bytes, for example) or by connect time. It would however, include any such fees where the value of the service lies in providing access to infringing material.” (Senate Report, p.44).
- c) Several courts have held that the mere ability to remove or block access to materials, or to exclude users, is not enough to constitute “right and ability to control” within the meaning of the DMCA safe harbors. *See Io Group v. Veoh Networks*, \_\_\_ F.Supp.2d \_\_\_, 2008 WL 4065872 at \*16 (N.D. Cal. Aug. 27, 2008) (“[T]he plain language of section 512(c) indicates that the pertinent inquiry is not whether Veoh has the right and ability to control its *system*, but rather, whether it has the right and ability to control the *infringing activity*.”); *Corbis v. Amazon*, 351 F. Supp. 2d 1090, 1110 (W.D. Wash. 2004); *Perfect 10 v. CCBill*, 340 F. Supp. 2d 1077, 1104 (C.D. Cal. 2004); *Perfect 10 v. Cybernet Ventures*, 213 F. Supp. 2d 1146, 1181-82 (C.D. Cal. 2002).
- d) One court has suggested that the “financial benefit” prong “should be interpreted consistent with the similarly-worded common law standard for vicarious copyright liability.” *See Perfect 10 v. CCBill*, 488 F.3d 1102, 1117 (9th Cir. 2007); *see also Io Group v. Veoh Networks*, \_\_\_ F.Supp.2d \_\_\_, 2008 WL 4065872 at \*15 (N.D. Cal. Aug. 27, 2008) (following *CCBill*). This interpretation is problematic to the extent it may render the safe harbors a dead letter as applied to vicarious liability claims, which is at odds with legislative history that indicates that the safe harbors were meant to reach those claims. *See Senate Report*, p.40 (safe harbors bar monetary damages for “direct, vicarious, or contributory infringement”).

#### D. Section 512(f): DMCA Misuse

1. Section 512(f) of the DMCA creates a cause of action for an OSP or end-user against “[a]ny person who knowingly materially misrepresents under this section (1) that material or activity is infringing, or (2) that material or activity was removed or disabled by mistake or misidentification.”
2. Those injured by misrepresentations in DMCA takedown notices are entitled to bring suit and recover actual damages, as well as costs and attorney’s fees. 17 U.S.C § 512(f).
3. “‘Knowingly’ means that a party actually knew, should have known if it acted with reasonable care or diligence, or would have had no substantial doubt had it been acting in good faith, that it was making misrepresentations.” *Online Policy Group v. Diebold, Inc.*, 337 F.Supp.2d 1195, 1204 (N.D.Cal. 2004) (finding misuse when DMCA notice targeted a clear fair use).
4. The Ninth Circuit has held that the “good faith” requirement in sending DMCA takedown notices “imposes a subjective good faith requirement upon copyright owners.” *Rossi v. Motion Picture Ass’n of America*, 391 F.3d 1000, 1004 (9th Cir. 2004) (interpreting “good faith” in § 512(c)(3)(A)(v)). “A copyright owner cannot be liable simply because an unknowing mistake is made, even if the copyright owner acted unreasonably in making the mistake. Rather, there must be a demonstration of some actual knowledge of misrepresentation on the part of the copyright owner.” *Id.* at 1005. This standard may prove problematic insofar as it appears to reward unreasonable mistakes on the part of copyright owners—the more unreasonable the person sending the takedown, seemingly the more leeway he would enjoy in sending takedowns. This seems at odds with Congress’ purpose in enacting § 512(f).
5. “‘Material’ means that the misrepresentation affected the ISP’s response to a DMCA letter.” *Id.*; see also *Rossi v. Motion Picture Ass’n of America*, 391 F.3d 1000 (9th Cir.2004); *Dudnikov v. MGA Entertainment, Inc.*, 410 F.Supp.2d 1010 (D. Colo. 2005) (“MGA was required to show that it had a sufficient basis to form the required good faith belief that the Plaintiffs’ auction infringed on its rights, and that its actions therefore complied with the notice and takedown requirements under the DMCA.”).
6. “[I]n order for a copyright owner to proceed under the DMCA with ‘a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law,’ the owner must evaluate whether the material makes fair use of the copyright. 17 U.S.C. § 512(c)(3)(A)(v). An allegation that a copyright owner acted in bad faith by issuing a takedown notice without proper consideration of the fair use doctrine thus is sufficient to state a misrepresentation claim pursuant to Section 512(f) of the DMCA.” *Lenz v. Universal Music Corp.*, \_\_\_ F.Supp.2d \_\_\_, 2008 WL 3884333 at \*3 (N.D. Cal. Aug. 20, 2008).

This document is licensed under the Creative Commons Attribution-Noncommercial-No Derivatives license, as described in full here: <<http://creativecommons.org/licenses/by-nc-nd/3.0/>>. Use consistent with this license requires no further permission from the author. Other reuse inquiries should be directed to Fred von Lohmann, [fred@eff.org](mailto:fred@eff.org).