

Congressional Research Service

Informing the legislative debate since 1914

Safe Harbor for Online Service Providers Under Section 512(c) of the Digital Millennium Copyright Act

Brian T. Yeh
Legislative Attorney

March 26, 2014

Congressional Research Service
7-5700
www.crs.gov
R43436

CRS REPORT
Prepared for Members and Committees of Congress

c11173008

Summary

Congress passed the Digital Millennium Copyright Act (DMCA) in 1998 in an effort to adapt copyright law to emerging digital technologies that potentially could be used to exponentially increase infringing activities online. Title II of the DMCA, titled the "Online Copyright Infringement Liability Limitation Act," added a new Section 512 to the Copyright Act (Title 17 of the U.S. Code) in order to limit the liability of providers of Internet access and online services that may arise due to their users posting or sharing materials that infringe copyrights. Congress was concerned that without insulating Internet intermediaries from crippling financial liability for copyright infringement, investment in the growth of the Internet could be stifled and innovation could be harmed.

The § 512 "safe harbor" immunity is available only to a party that qualifies as a "service provider" as defined by the DMCA, and only after the provider complies with certain eligibility requirements. The DMCA's safe harbors greatly limit service providers' liability based on the specific functions they could perform: (1) transitory digital network communications, (2) system caching, (3) storage of information on systems or networks at direction of users, and (4) information location tools. In exchange for the shelter from most forms of liability, the DMCA requires service providers to cooperate with copyright owners to address infringing activities conducted by the providers' customers. The safe harbor thus reflects a "grand bargain" between creative content-producing industries and Internet companies that seeks to both promote investment in the Internet and protect copyright holders' intellectual property rights.

The DMCA expressly states that a service provider is not required to actively monitor its service for infringing activity. However, § 512 requires a service provider, upon proper notification by the copyright owner of online material being displayed or transmitted without authorization, to "expeditiously" remove or disable access to the allegedly infringing material. In addition, a service provider must remove or disable access to material upon acquiring actual knowledge that materials or activities on its system or network are infringing (for example, actual knowledge can be obtained by the copyright holder's notification) *or* when the service provider becomes aware of facts or circumstances from which infringing activity is apparent (so-called "red flag" knowledge). Service providers that meet the eligibility conditions of the § 512 safe harbor are thus shielded from liability for *unknowingly* hosting content that infringes copyrights, whereas § 512 provides copyright holders a simple and cost-effective procedural mechanism for remedying online infringement of their intellectual property rights. Courts have found that the burden of actively monitoring online copyright infringement lies on copyright holders.

This report focuses primarily on the third safe harbor functional category, "storage of information on systems or networks at direction of users," which includes any website that stores digital content that users have uploaded for public consumption or for sharing purposes, such as popular social media and online services YouTube, Facebook, Dropbox, Flickr, Google Drive, and Blogger. The report will describe and analyze the statutory language establishing the safe harbor as well as discuss federal court cases that have considered the scope and application of the DMCA safe harbors and the extent to which online service providers can be held indirectly liable for copyright infringement committed by their users.

c11173008

Contents

Introduction 1
Background 2
Secondary Liability for Copyright Infringement 3
User Generated Content and the Internet 4
Safe Harbor Provisions 5
Eligibility Threshold for Any Safe Harbor 5
Requirements for Each Safe Harbor 6
§ 512(a) Transitory Digital Network Communications 6
§ 512(b) System Caching 6
§ 512(c) Information Residing on Systems or Networks at Direction of Users 7
§ 512(d) Information Location Tools 8
Takedown Notices 8
Limited Injunctive Relief Still Possible 9
Judicial Interpretations of the § 512(c) Safe Harbor 9
Burden of Policing Infringement 10
Definition of "Storage" 10
Repeat Infringer Termination Policy 11
Notification Requirement 11
Actual Knowledge of Infringement 12
"Red Flag" Apparent Knowledge of Infringement 13
Willful Blindness 14
"Right and Ability to Control" Infringing Activity 15
Recent Legislative Activities 16

Contacts

Author Contact Information 16

c11173008

Introduction

Online service providers (OSPs) and Internet service providers (ISPs) provide critical infrastructure support to the Internet, allowing millions of people to access online content and electronically communicate and interact with each other. The potential for computer users to infringe intellectual property rights using the Internet, specifically copyrights, could expose "intermediary" service providers to claims of secondary liability, such as contributory and vicarious copyright infringement. Concerned about this significant legal vulnerability of service providers, Congress passed the "Online Copyright Infringement Liability Limitation Act," Title II of the Digital Millennium Copyright Act (DMCA) of 1998,[1] in an effort to adapt copyright law to an evolving digital environment.[2] The act added a new Section 512 to the Copyright Act (Title 17 of the U.S. Code), which provides limitations on the liability of OSPs and ISPs against claims of copyright infringement arising from their users' activities on their digital networks.[3]

The act's legislative history indicates that Congress wanted to provide service providers with "more certainty ... in order to attract the substantial investments necessary to continue the expansion and upgrading of the Internet."[4] At the same time, Congress desired to preserve "strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment."[5] The DMCA therefore includes several conditions that the service provider must satisfy in order to qualify for § 512 "safe harbor" protection from most infringement liability, and requires that the service providers' activities be encompassed within one of four specified categories of conduct. The safe harbors correspond to the following four functional operations that might otherwise constitute copyright infringement: (1) transitory digital network communications, (2) system caching, (3) storage of information on systems or networks at direction of users, and (4) information location tools.[6]

One federal district court assessed the "dual purpose and balance" of § 512 in the following manner:

> Congress created tradeoffs within the DMCA: service providers would receive liability protections in exchange for assisting copyright owners in identifying and dealing with infringers who misuse the service providers' systems. At the same time, copyright owners would forgo pursuing service providers for the copyright infringement of their users, in exchange for assistance in identifying and acting against those infringers.[7]

A public interest group has praised the importance of the DMCA's safe harbor provisions to the development of the Internet:

---

[1] P.L. 105-304, 112 Stat. 2860 (1998) (codified at 17 U.S.C. § 512).

[2] *See* Ellison v. Robertson, 357 F.3d 1072, 1076 (9th Cir. 2004).

[3] The Digital Millennium Copyright Act of 1998: U.S. Copyright Office Summary, 8 (Dec. 1998) at http://www.copyright.gov/legislation/dmca.pdf. (Hereinafter "Copyright Office Summary.")

[4] 144 CONG. REC. S11,889 (daily ed. Oct. 2, 1998) (statement of Sen. Hatch).

[5] H.Rept. 105-796, 105th Cong., 2d Sess. 72 (1998).

[6] 17 U.S.C. § 512(a)-(d).

[7] In re Verizon Internet Servs., Inc., 240 F. Supp. 2d 24, 37 (D.D.C. 2003), *rev'd sub nom*. Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003).

c11173008

> Without these protections, the risk of potential copyright liability would prevent many online intermediaries from providing services such as hosting and transmitting user-generated content. Thus the safe harbors have been essential to the growth of the Internet as an engine for innovation and free expression.[8]

Although all four safe harbors will be described at the beginning of this report, the primary focus for the rest of the report will be on the third category that encompasses the function of many popular Internet businesses today: "storage of information on systems or networks at direction of users." This safe harbor is essential to the business model of most ISPs and OSPs that permit user generated content (UGC) to be stored or shared using their networks.

Background

Copyright is a federal grant of legal protection available to the creator or owner of certain original works of creative expression, including books, movies, photography, art, and music.[9] A copyright holder possesses several exclusive legal entitlements under the Copyright Act, which together provide the holder with the right to determine whether and under what circumstances the protected work may be used by third parties. The grant of copyright permits the copyright holder to authorize or refuse to authorize others to exercise the following exclusive rights:

- the reproduction of the copyrighted work;
- the preparation of derivative works based on the copyrighted work;
- the distribution of copies of the copyrighted work;
- the public performance of the copyrighted work; and
- the public display of the copyrighted work, including the individual images of a motion picture.[10]

Therefore, a party desiring to reproduce, adapt, distribute, publicly display, or publicly perform a copyrighted work must either (1) obtain the permission of the copyright holder (usually granted in the form of a license agreement that establishes conditions of use and an amount of monetary compensation known as a royalty fee); (2) comply with the terms of compulsory licenses established by law;[11] or (3) assert that such use falls within the scope of certain statutory limitations on the exclusive rights such as the "fair use" doctrine—but the validity of such claim may be subject to the judgment of a federal court.[12]

Each exclusive right of a copyright holder is potentially subject to licensing; for example, a third party wishing to reproduce a copyrighted work as well as publicly perform the work must negotiate separate licenses from the copyright holder to engage in the different activities.

---

[8] Electronic Frontier Foundation, *Digital Millennium Copyright Act*, *at* http://www.eff.org/issues/dmca.

[9] 17 U.S.C. § 102(a).

[10] 17 U.S.C. § 106.

[11] "Statutory" or "compulsory" licenses compel copyright owners to allow third parties to use creative works under certain conditions and according to specific requirements, in exchange for payment of royalty fees at a rate determined by a federal government body known as the Copyright Royalty Board.

[12] 17 U.S.C. § 107.

c11173008

Unauthorized use of a copyrighted work by a third party in a manner that implicates one of the copyright holder's exclusive rights constitutes infringement.[13] The copyright holder may file a lawsuit in federal court against an alleged infringer for a violation of any of the exclusive rights conferred by copyright. The Copyright Act provides several civil remedies to the copyright holder that is harmed by infringement, including the possibility of obtaining injunctive relief,[14] actual damages suffered by the copyright owner due to the infringement,[15] statutory damages,[16] and costs and attorney fees.[17]

The rights conferred by a copyright do not last forever. Copyrights are limited in the number of years a copyright holder may exercise his/her exclusive rights. In general, an author of a creative work may enjoy copyright protection for the work for a term lasting the entirety of his/her life plus 70 additional years.[18] At the expiration of a term, the copyrighted work becomes part of the public domain. A work in the public domain is available for anyone to use without the need to seek prior permission of the creator of the work.

Secondary Liability for Copyright Infringement

Someone who *directly* infringes a copyright is not the only party potentially liable for infringement; one who significantly "aids and abets" another party's commission of a direct infringement may also be sued by the rights holder for *indirect*, or secondary, infringement. The concept of secondary infringement has its roots in tort law and the notion that one should be held accountable for directly contributing to another's infringement.[19] The federal courts have recognized secondary infringement liability in copyright and trademark law, while the Patent Act contains provisions that expressly authorize it.[20] Because online service providers often solely provide the means for their users to upload and distribute content, rather than providing the content themselves, service providers are more likely to be charged with secondary infringement liability rather than sued for direct infringement.

In copyright law, there are three common theories of indirect infringement liability: contributory, vicarious, and inducement liability. For contributory copyright infringement liability to exist, a court must find that the secondary infringer "with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another."[21] "Vicarious" infringement liability in copyright law is possible where a defendant "has the right and ability to supervise the

[13] 17 U.S.C. § 501.

[14] 17 U.S.C. § 502.

[15] 17 U.S.C. § 504(b).

[16] 17 U.S.C. § 504(c)(1).

[17] 17 U.S.C. § 505.

[18] 17 U.S.C. § 302. Other terms have been established for different works and different periods of time. For a concise chart explaining the different terms, *see* http://www.copyright.cornell.edu/resources/publicdomain.cfm.

[19] Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996).

[20] The Supreme Court in *Sony Corp. of Am. v. Universal City Studios, Inc.,* 464 U.S. 417, 435 (1984) stated: "The absence of such express language in the copyright statute does not preclude the imposition of liability for copyright infringements on certain parties who have not themselves engaged in the infringing activity. For vicarious liability is imposed in virtually all areas of the law, and the concept of contributory infringement is merely a species of the broader problem of identifying the circumstances in which it is just to hold one individual accountable for the actions of another."

[21] A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1019 (9th Cir. 2001).

c11173008

infringing activity and also has a direct financial interest in such activities."[22] In 2005, the U.S. Supreme Court expressly adopted a relatively new theory of secondary infringement in copyright cases referred to as "inducement liability." In *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.,* the Court articulated the standard for inducement liability:

> [O]ne who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties. ... [M]ere knowledge of infringing potential or of actual infringing uses would not be enough here to subject a distributor to liability. ... The inducement rule, instead, premises liability on purposeful, culpable expression and conduct... [23]

User Generated Content and the Internet

Copyright protection extends to electronic documents, videos, photos, music, and other copyrightable subject matter that may be accessible via the Internet. Uploading and downloading copyrighted works without the authorization of the copyright holders is generally a violation of the copyright holders' exclusive rights to control, respectively, the distribution and reproduction of their works.[24] However, the fair use doctrine may apply to materials that are posted on websites—that is, someone accused of online copyright infringement may be able to assert fair use to escape liability; as explained above, however, a federal court would need to determine whether the use of such material on a website qualifies as a fair use.

Several types of Internet technologies enable the storage and sharing of "user generated content" (UGC), which is digital content (such as documents, photographs, music, and video) that is supplied by Internet end-users. Many Internet businesses rely on their users to upload and share UGC to further interest in and usage of their websites or software. In most cases, the UGC is protected by copyright (whether owned by the user or a third party), although online posting or sharing of the material may be authorized by the copyright holder (for promotional purposes, for example), the copyright holder may not object to the posting, or the particular unauthorized activity could nevertheless qualify for a liability defense such as "fair use."

A commonly used UGC technology is the "cyberlocker" or "file hosting service," which provides online storage in the Internet "cloud" for users' digital files. After users have uploaded their files to the online storage location, they may access them from mobile devices or other computers as well as share them publicly or with designated friends and coworkers. Dropbox, Google Drive, YouTube, Facebook, and Instagram are all examples of such cyberlocker services. Although these services all require their users to agree to "Terms of Use" or "Terms of Service" that specifically prohibit the uploading of copyrighted content which they do not have the legal right to post, users often violate these terms by engaging in the unauthorized uploading and sharing of copyrighted music files, television shows, and movies.

[22] Gershwin Publ'g Corp. v. Columbia Artists Mgmt, Inc., 443 F2d. 1159, 1162 (2d. Cir. 1971).

[23] 545 U.S. 913 (2005).

[24] *Id.* at 923; *see also* Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1034 (9th Cir. 2013).

c11173008

Safe Harbor Provisions

Limitations on liability, often called "safe harbors," shelter service providers from copyright infringement suits. The DMCA's safe harbor provisions, codified at 17 U.S.C. § 512, do not confer absolute immunity, but they do significantly limit service providers' liability based on the specific functions they perform.[25] The safe harbors correspond to four functional operations of a service provider: (1) transitory digital network communications, (2) system caching, (3) storage of information on systems or networks at direction of users, and (4) information location tools.[26]

Eligibility Threshold for Any Safe Harbor

For protection under any of the safe harbor provisions, a party must first meet the statutory definition of a "service provider." The DMCA provides two distinct definitions, one applicable to the first safe harbor category and the second applicable to all of the others. Under § 512(a), the transitory communications provision, "service provider" is narrowly defined as "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."[27] The remaining three subsections utilize a broader definition of "service provider," applicable to "a provider of online services or network access, or the operator of facilities therefor."[28] For example, this definition encompasses providers offering "Internet access, e-mail, chat room and web page hosting services."[29]

After a party qualifies as a service provider under one of the applicable definitions, there are still two additional threshold requirements that the provider must satisfy:[30]

- The service provider must have adopted, reasonably implemented, and informed its users of a "repeat infringer" policy for the termination of the accounts of subscribers who are repeat copyright infringers.
- The provider must accommodate, and not interfere with, "standard technical measures"[31] that are used by copyright owners to identify or protect their works, such as digital watermarks on photographs or digital rights management technologies embedded in videos.

In addition to the three threshold criteria listed above, a service provider must satisfy the specific requirements of the particular safe harbor in question, which are described in the section below.

---

[25] Ellison v. Robertson, 189 F. Supp. 2d 1051, 1064 (C.D. Cal. 2002), *aff'd in part and rev'd in part*, 357 F.3d 1072 (9th Cir. 2004). Service providers who qualify for safe harbor are protected from all monetary and most equitable relief that may arise from copyright liability. In such a situation, "even if a plaintiff can show that a safe harbor-eligible service provider has violated her copyright, the plaintiff will only be entitled to the limited injunctive relief set forth in 17 U.S.C. § 512(j)." Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1098-99 (W.D. Wash. 2004) (citations omitted).

[26] 17 U.S.C. § 512(a)-(d).

[27] 17 U.S.C. § 512(k)(1)(A).

[28] 17 U.S.C. § 512(k)(1)(B).

[29] H.Rept. 105-551, pt. 2 at 64.

[30] 17 U.S.C. § 512(i)(1)(A)-(B).

[31] "Standard technical measures" is defined at § 512(i)(2).

c11173008

Note that qualification for any one of these safe harbors is limited to the criteria detailed in each safe harbor provision, and qualification under one safe harbor category does not affect the eligibility determination for any of the other three.[32]

Requirements for Each Safe Harbor

§ 512(a) Transitory Digital Network Communications

When a service provider acts as a data conduit at the request of a third party by "transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider," it will be shielded from liability for copyright infringement.[33] This safe harbor also protects the service provider for any intermediate and transient storage of the material in the course of conveying the digital information. However, qualification for this safe harbor is subject to several conditions, including the following:[34]

- Data transmission occurs through an automated technical process without selection of the material by the service provider.
- The service provider does not determine the recipients of the material.
- Intermediate or transient copies stored on the provider's system or network must not be accessible to anyone other than the designated recipients, and such copies must not be retained on the system longer than is reasonably necessary.
- The provider must not have modified the content of the transmitted material.

§ 512(b) System Caching

The second safe harbor category limits ISP liability when it engages in "caching" of online content for purposes of improving network performance. Caching[35] helps to reduce the service provider's network congestion and increase download speeds for subsequent requests for the same data. For example, subscribers to a service provider may transmit certain material to other users of the provider's system or network, at the direction of those users. The service provider may, via an automated process, retain copies of this material for a limited time "so that subsequent requests for the same material can be fulfilled by transmitting the retained copy, rather than retrieving the material from the original source on the network."[36] Immunity for service providers that utilize system caching is provided on the condition that the ISP complies with the following:[37]

- The content of cached material that is transmitted to subsequent users is not modified by the service provider.

[32] 17 U.S.C. § 512(n).

[33] 17 U.S.C. § 512(a).

[34] *Id.*

[35] Caching is defined as "intermediate and temporary storage of material on a system or network operated by the service provider." 17 U.S.C. § 512(b).

[36] *Copyright Office Summary,* at 10.

[37] 17 U.S.C. § 512(b)(2)(A)-(E).

c11173008

- The provider complies with industry standard rules regarding the refreshing, reloading, or other updating of the cached material.
- The provider does not interfere with the ability of technology that returns "hit" count information that would otherwise have been collected had the website not been cached to the person who posted the material.
- The provider must impose the same conditions that the original poster of the material required for access, such as passwords or payment of a fee.
- The provider must remove or block access to any material that is posted without the copyright owner's authorization, upon being notified that such material has been previously removed from the originating site, or that the copyright owner has obtained a court order for the material to be removed from the originating site or to have access to the material be disabled.

§ 512(c) Information Residing on Systems or Networks at Direction of Users

This safe harbor, which is the primary focus of this report, protects against copyright infringement claims due to storage of infringing material at the direction of a user on ISP systems or networks. Such storage includes "providing server space for a user's website, for a chat room, or other forum in which material may be posted at the direction of users."[38] The conditions placed on receiving the benefit of this safe harbor are as follows:[39]

- The service provider lacks actual knowledge of the infringing material hosted or posted on its system or network.
- In the absence of actual knowledge, the service provider is "not aware of facts or circumstances from which infringing activity is apparent."[40]
- Upon obtaining either actual knowledge or awareness of infringing material, the service provider must "act[] expeditiously to remove, or disable access to, the material."[41]
- Where the provider has the right and ability to control the infringing activity, it must not derive a financial benefit directly attributable to that activity.
- Upon receiving proper notification of claimed infringement, the service provider must act "expeditiously" to remove or block access to the material.
- The service provider must designate an agent to receive notifications of claimed infringement. The contact information for this agent must be filed with the Register of Copyrights[42] and also be displayed to the public on the service provider's website.

[38] H.Rept. 105-551, pt. 2, 105th Cong. 2d Sess. 53 (1998).

[39] 17 U.S.C. § 512(c).

[40] 17 U.S.C. § 512(c)(1)(A)(ii).

[41] 17 U.S.C. § 512(c)(1)(A)(iii).

[42] "The Register of Copyrights is directed to maintain a directory of designated agents available for inspection by the public, both on the website of the Library of Congress, and in hard copy format on file at the Copyright Office." H.Rept. 105-551, pt. 2 at 55.

c11173008

- Copyright owners must adhere to a prescribed procedure to inform the provider's designated agent of claimed infringement. To constitute effective notification, the copyright owner must "comply substantially" with the statutory requirements of § 512(c)(3):[43]
  1. The notification is in writing, signed physically or electronically by a person authorized to act on behalf of the owner of the copyright allegedly infringed.
  2. The notification identifies the material that is claimed to have been infringed and provides sufficient information allowing the service provider to locate the material.
  3. The complaining party includes a statement, under penalty of perjury, that the party has a "good faith belief" that the use of the material is not authorized by the copyright owner, and that the information in the notification is accurate.

§ 512(d) Information Location Tools

The fourth safe harbor classification immunizes service providers that provide users access to websites that contain infringing material by using "information location tools" such as hypertext links, indexes, and directories.[44] The conditions attached are substantially similar to those that apply to the "system storage" safe harbor provision discussed above, § 512(c), including lack of actual or constructive knowledge requirements, notice and take-down procedures, and absence of direct financial benefit.[45] The rationale for protecting service providers under this provision is to promote development of the search tools that make finding information possible on the Internet.[46] Without a safe harbor for providers of these tools, the human editors and cataloguers compiling Internet directories might be overly cautious for fear of being held liable for infringement.

Takedown Notices

One condition common to three of the four categories is the requirement that upon proper notification by the copyright owner of online material being displayed or transmitted without authorization, a service provider must "expeditiously" remove or disable access to the allegedly infringing material.[47] This "notice and takedown" obligation does not apply when the service provider functions as a passive conduit of information under § 512(a), but is a condition that must be met to obtain shelter under the remaining three safe harbor provisions. As indicated by the eligibility conditions in each subsection of § 512(b)-(d), the notice and takedown procedure varies slightly for each.

To prevent abuse of the notice and takedown procedure, § 512(f) provides damages, costs, and attorneys' fees to any service provider that is injured by a knowing, material misrepresentation that an item or activity is infringing.[48] For example, any person who sends a "cease and desist"

[43] 17 U.S.C. § 512(c)(3)(A)(i)-(vi).

[44] 17 U.S.C. § 512(d).

[45] 17 U.S.C. § 512(d)(1)-(3).

[46] H.Rept. 105-551, pt. 2 at 58.

[47] *See* 17 U.S.C. § 512(b)(E), (c)(C), and (d)(3).

[48] "'Knowingly' means that a party actually knew, should have known if it acted with reasonable care or diligence, or (continued...)

c11173008

letter to a service provider, with the knowledge that the claims of copyright infringement are false, may be liable to the accused infringer for damages.

Limited Injunctive Relief Still Possible

As noted earlier, the DMCA's safe harbor provisions do not confer absolute immunity from legal liability for copyright infringement. Although they ensure that qualifying service providers are not liable for monetary damages, service providers may still be liable for certain injunctive relief. For example, in the case of service providers that provide either (1) system caching, (2) storage of information on systems or networks at direction of users, or (3) information location tools, the court may grant injunctive relief with respect to a service provider in one or more of the following forms:

- 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;
- 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;
- such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified 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.[49]

Judicial Interpretations of the § 512(c) Safe Harbor

Since the enactment of the DMCA, many online service providers have been the target of infringement lawsuits by large companies that own copyrighted content, particularly recorded music, television shows, and motion pictures. These lawsuits typically accuse the service provider of direct, vicarious, and contributory copyright infringement, as well as inducement of infringement. The cases often begin by the service provider asserting a DMCA safe harbor as an affirmative defense that limits its infringement liability; as an affirmative defense, the service provider has the burden of establishing that it meets the safe harbor's eligibility requirements.[50] If this burden is satisfied, courts often find for the defendant on summary judgment. It is important to keep in mind that a service provider's inability to qualify for a safe harbor does not mean that it is presumptively liable for copyright infringement; rather, the copyright holder must still prove its infringement claim.

(...continued)

would have had no substantial doubt had it been acting in good faith, that it was making misrepresentations. 'Material' means that the misrepresentation affected the ISP's response to a DMCA letter." Online Policy Group v. Diebold, Inc., 337 F. Supp. 2d 1195, 1204 (N.D. Cal. 2004) (citations omitted).

[49] 17 U.S.C. § 512(j)(1)(A).

[50] *See* Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1039 (9th Cir. 2013).

c11173008

Through the many cases in which the § 512(c) safe harbor is asserted as protecting a service provider from some forms of infringement liability, the federal courts have had an opportunity to interpret the statutory language and evaluate the scope of the safe harbor's application. What follows is a discussion of these cases.

Burden of Policing Infringement

Section 512(m) expressly provides that the DMCA's safe harbor provisions are not conditioned upon a service provider "monitoring its service or affirmatively seeking facts indicating infringing activity."[51] The federal courts generally agree that the DMCA imposes the duty to police infringement on the copyright holders, not the service providers. In *Perfect 10, Inc. v. CCBill LLC,* the Ninth Circuit Court of Appeals explained that

> The DMCA notification procedures place the burden of policing copyright infringement—identifying the potentially infringing material and adequately documenting infringement—squarely on the owners of the copyright. We decline to shift a substantial burden from the copyright owner to the provider... [52]

The district court in *Viacom International, Inc. v. YouTube, Inc.,* agreed with the *Perfect 10* appellate court, remarking that placing the burden on the copyright holder to monitor for infringing activity

> makes sense, as the infringing works in suit may be a small fraction of millions of works posted by others on the service's platform, whose provider cannot by inspection determine whether the use has been licensed by the owner, or whether its posting is a "fair use" of the material, or even whether its copyright owner or licensee objects to its posting.[53]

Definition of "Storage"

In *Viacom International, Inc. v. YouTube, Inc.,* the large media conglomerate Viacom argued (among many other things) that YouTube, the most popular video-sharing website, did not qualify for the § 512(c) safe harbor because it replicates, transmits, and displays videos, rather than merely "stores" the UGC. The district court disagreed with Viacom's proposed narrow definition of "storage," and explained that the statutory definition of "service provider" is defined as "a provider of online services or network access, or the operator of facilities therefor," and includes "an entity offering the transmission, routing, or providing of connections for digital online communications."[54] Thus, the court held that the "collateral scope" of "storage" includes YouTube's offering of software functions that facilitate user access to the UGC, which include reproduction, display, or performance of the videos.[55]

---

[51] 17 U.S.C. § 512(m)(1).

[52] 488 F.3d 1102, 1113 (9th Cir. 2007).

[53] 718 F. Supp. 2d 514, 524 (S.D.N.Y. 2010).

[54] *Id.* at 526, *citing* 17 U.S.C. § 512(k)(1)(B).

[55] *Id.* at 527. *See also* UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1016 (9th Cir. 2013) (finding that the § 512(c) safe harbor extends to infringement resulting not just from the provider's storage of UGC, but also any services that the provider operates to facilitate users' access to the material).

c11173008

Repeat Infringer Termination Policy

In *Ellison v. Robertson,*[56] the defendant service provider was denied safe harbor protection for failure to meet the threshold eligibility requirements under § 512(i), the "repeat infringer termination policy" provision. Stephen Robertson had electronically scanned and converted into digital files several science fiction novels written by Harlan Ellison, without authorization of the copyright owner. Robertson then uploaded and copied the files onto newsgroups that are carried by several ISPs, including America Online, Inc. (AOL). Once Ellison learned of the infringing activity, he e-mailed a notice of copyright infringement pursuant to the DMCA notification procedures. AOL, however, claimed never to have received the notice. Receiving no response, the plaintiff then filed a copyright infringement suit against AOL and other parties.

The Ninth Circuit Court of Appeals reversed the district court's conclusion that AOL qualified for a safe harbor limitation of liability. The appellate court found "at least a triable issue of material fact" regarding AOL's threshold eligibility for safe harbor under § 512(i).[57] First, the court explained that § 512(i)(1)(A) has three separate requirements for a service provider to fulfill:

- Adopt a policy that provides for the termination of service access for repeat copyright infringers in appropriate circumstances.
- Inform users of the service policy.
- Implement the policy in a reasonable manner.

The court determined that there was "ample evidence in the record" to suggest that AOL failed to satisfy the last of these requirements. Because AOL had changed the e-mail address to which infringement notifications were being sent and did not close the old e-mail account or forward the messages to the new address, "AOL allowed notices of potential copyright infringement to fall into a vacuum and to go unheeded."[58] This fact alone provides a basis for a reasonable jury to find that AOL did not "reasonably implement[]" a policy against repeat infringers.[59]

Notification Requirement

In *ALS Scan, Inc. v. RemarQ Communities, Inc.*, the Fourth Circuit Court of Appeals considered whether a service provider is eligible for protection when it is alerted to infringing activity by "imperfect notice" that does not strictly comply with the notification procedures specified in § 512(c)(3).[60] ALS Scan holds the copyrights to over 10,000 "adult" photographs which were posted on newsgroups that were operated by the service provider RemarQ Communities. Upon discovering that RemarQ's servers contained infringing material, ALS Scan sent a "cease and desist" letter to RemarQ, requesting deletion of two specific newsgroups that contained the photographs. However, the district court in *ALS Scan* found that the notice was "fatally defective" in complying with § 512(c)(3) because ALS Scan never provided RemarQ with a "representative list" of the infringing photographs. Nor did it identify the pornographic photographs with

[56] 357 F.3d 1072 (9th Cir. 2004)

[57] *Id.* at 1080.

[58] *Id.*

[59] *Id.*

[60] 239 F.3d 619, 620 (4th Cir. 2001).

c11173008

"sufficient detail" to enable RemarQ to locate and disable access to them.[61] In reversing the district court's ruling granting summary judgment in favor of RemarQ, the court of appeals held that ALS Scan had "substantially complied" with DMCA notification requirements because its notice letter identified by name the two RemarQ newsgroup sites "created solely for the purpose of publishing and exchanging ALS Scan's copyrighted images" and also referred RemarQ to website addresses where RemarQ could find pictures and names of ALS Scan's adult models.[62] Thus, the court of appeals held that since RemarQ was provided with a notice that *substantially* complied with the DMCA, the service provider could not rely on a claim of defective notice to maintain the safe harbor defense.[63]

Actual Knowledge of Infringement

The DMCA requires a service provider to remove or disable access to material upon obtaining "actual knowledge that the material or an activity using the material on the system or network is infringing."[64] (A service provider may also choose to ignore its actual knowledge of infringement, but doing so would render it ineligible for safe harbor protection.) A mere "generalized awareness" of infringement, even if it may be prevalent throughout its digital network or system, does not impose a legal duty on a service provider to monitor or search for infringements.[65] Rather, a service provider must have "knowledge of specific and identifiable infringements of particular individual items" before the legal duty is triggered.[66] The Second Circuit Court of Appeals in *Viacom International, Inc. v. YouTube, Inc.* reasoned that "the nature of the removal obligation itself contemplates knowledge or awareness of specific infringing material, because expeditious removal is possible only if the service provider knows with particularity which items to remove."[67]

In *Corbis Corp. v. Amazon.com, Inc.*,[68] the federal district court determined that the electronic commerce company Amazon.com had qualified for safe harbor with regard to infringing activity allegedly occurring in its zShops third-party vendor service.[69] Corbis, a company that licenses art images and celebrity photographs, had sued Amazon, claiming that several hundred images in which it had a "copyright interest" were being copied, displayed, and sold through Amazon's

[61] *Id.* at 624.

[62] *Id.* at 624-25. The court further explained, "[W]hen a letter provides notice equivalent to a list of representative works that can be easily identified by the service provider, the notice substantially complies with the notification requirements." *Id.* at 625.

[63] *Id.* at 620 (emphasis in original).

[64] 17 U.S.C. § 512(c)(1)(A)(i), (iii).

[65] Viacom Int'l, Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 523-24 (S.D.N.Y. 2010) ("To let knowledge of a generalized practice of infringement in the industry, or of a proclivity of users to post infringing materials, impose responsibility on service providers to discover which of their users' postings infringe a copyright would contravene the structure and operation of the DMCA.").

[66] *Id.* at 523. *See also* Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 26 (2d Cir. 2012) (hold that "the District Court correctly held that the § 512(c) safe harbor requires knowledge or awareness of specific infringing activity.").

[67] *Id.* at 30.

[68] 351 F. Supp. 2d 1090 (W.D. Wash. 2004).

[69] "The zShops platform allows individuals and retailers (referred to as 'vendors') to showcase their products and sell them directly to online consumers. Amazon, however, does not sell any of its own inventory on the zShops platform." Id. at 1094.

c11173008

zShops sites.[70] Amazon sought liability protection under the § 512(c) safe harbor. The court found that Amazon did not have actual knowledge that material on its network is infringing because Corbis, prior to filing the lawsuit, had never attempted to notify Amazon about the alleged infringing conduct of zShop vendors. Thus, the court explained, Corbis missed its opportunity to provide "the most powerful evidence of a service provider's knowledge–actual notice of infringement from the copyright holder."[71]

In *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, Universal Music Group (UMG), one of the largest recorded music and music publishing companies, sued Veoh Networks, an operator of a website that allowed users to share videos with others.[72] First, the Ninth Circuit Court of Appeals observed that UMG had not notified Veoh of any specific infringing video on its system and thus, like Corbis Corporation, the failure to use the formal DMCA notice protocol "stripped it of the most powerful evidence of a service provider's knowledge."[73] UMG argued, however, that Veoh, by hosting a category of copyrighted content such as "music videos" for which it had no license from any major music company, had actual knowledge of the infringing material on its website.[74] The appellate court rejected this proposition, holding that with only the "general knowledge that one's services could be used to share infringing material," a service provider lacks actual knowledge of infringement.[75]

"Red Flag" Apparent Knowledge of Infringement

In the absence of "actual knowledge" that materials or activities on their system or network are infringing, a service provider has an obligation to "expeditiously" remove or disable access to infringing content when it becomes "aware of facts or circumstances from which infringing activity is apparent."[76] The service provider's duty to remove material upon obtaining an "awareness" of apparent infringing activity is the so-called "red flag" provision of the DMCA and it is distinct from the "actual knowledge" requirement discussed in the previous section.

In *Perfect 10 Inc. v. CCBill LLC,* the Ninth Circuit Court of Appeals disagreed with the plaintiff's allegation that the defendants (who provided web hosting services to other websites) had received notice of apparent infringement from "red flags" such as websites that were named "illegal.net" and "stolencelebritypics.com."[77] The appellate court explained that "[w]hen a website traffics in pictures that are titillating by nature, describing photographs as 'illegal' or 'stolen' may be an attempt to increase their salacious appeal, rather than an admission that the photographs are actually illegal or stolen. We do not place the burden of determining whether photographs are actually illegal on a service provider."[78]

[70] *Id*. at 1096-97.

[71] *Id*. at 1107.

[72] UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013).

[73] *Id.* at 1020, *citing Corbis Corp. v. Amazon.com, Inc.,* 351 F. Supp. 2d 1090 (W.D. Wash. 2004).

[74] *Id.* at 1021.

[75] *Id.* at 1022.

[76] 17 U.S.C. § 512(c)(1)(A)(ii), (iii).

[77] 488 F.3 1102, 1114 (9th Cir. 2007).

[78] *Id.*

c11173008

The appellate court in *Viacom International, Inc. v. YouTube, Inc.* described the difference between actual knowledge and "red flag knowledge" as being "between a subjective and an objective standard:"

> [T]he actual knowledge provision turns on whether the provider actually or "subjectively" knew of specific infringement, while the red flag provision turns on whether the provider was subjectively aware of facts that would have made the specific infringement "objectively" obvious to a reasonable person. The red flag provision, because it incorporates an objective standard, is not swallowed up by the actual knowledge provision under our construction of the § 512(c) safe harbor. Both provisions do independent work, and both apply only to specific instances of infringement.[79]

Willful Blindness

The doctrine of willful blindness is used widely within the federal judiciary in criminal law cases involving criminal statutes that require proof that a defendant acted knowingly or willfully, in order to hold defendants accountable so that they "cannot escape the reach of these statutes by deliberately shielding themselves from clear evidence of critical facts that are strongly suggested by the circumstances."[80] The Supreme Court has previously explained that "persons who know enough to blind themselves to direct proof of critical facts *in effect* have actual knowledge of those facts."[81]

In a case examining induced patent infringement liability, *Global-Tech Appliances, Inc. v. SEB S.A.,*[82] the Supreme Court described a two-part test for the willful blindness doctrine:

1. The defendant must subjectively believe that there is a high probability that a fact exists.
2. The defendant must take deliberate actions to avoid learning of that fact.[83]

The Court believed that these two requirements of the willful blindness doctrine provide "an appropriately limited scope that surpasses recklessness and negligence."[84] The differences between these three standards, according to the Court, are as follows:

- "[A] willfully blind defendant is one who takes deliberate actions to avoid confirming a high probability of wrongdoing and who can almost be said to have actually known the critical facts."
- "[A] reckless defendant is one who merely knows of a substantial and unjustified risk of such wrongdoing."
- "[A] negligent defendant is one who should have known of a similar risk but, in fact, did not."[85]

---

[79] Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 31 (2d Cir. 2012).

[80] Global-Tech Appliances, Inc. v. SEB S.A., 131 S. Ct. 2060, 2068-69 (2011).

[81] *Id.* at 2069 (emphasis added).

[82] For more information on this decision, *see* CRS Report R41976, *Intent Standard for Induced Patent Infringement: Global-Tech Appliances, Inc. v. SEB S.A.* , by Brian T. Yeh.

[83] *Global-Tech,* 131 S. Ct. at 2070 (citing various opinions of the Courts of Appeals that have articulated the doctrine).

[84] *Id.*

c11173008

The Second Circuit Court of Appeals in *Viacom International, Inc. v. YouTube, Inc.* was the first appellate court to consider the application of the common law willful blindness doctrine in the DMCA context. The court acknowledged that the DMCA does not expressly mention willful blindness. Nevertheless, the court held that the doctrine could apply in certain circumstances "to demonstrate knowledge or awareness of specific instances of infringements under the DMCA,"[86] for example, if a service provider makes deliberate efforts to avoid obtaining knowledge of specific infringing activity.

The Ninth Circuit Court of Appeals in *UMG Recordings, Inc. v.* Shelter Capital Partners LLC also agreed with the *Viacom* appellate court that "a service provider cannot willfully bury its head in the sand to avoid obtaining such specific knowledge."[87] However, in the case at hand, the court found "no evidence that Veoh acted in such a manner," but instead noted that "Veoh promptly removed infringing material when it became aware of specific instances of infringement."[88]

"Right and Ability to Control" Infringing Activity

Section 512(c)(1)(B) specifies that for a service provider to be eligible for the safe harbor applicable to online storage functions, the provider must not receive a "financial benefit directly attributable to the infringing activity" that it has the "right and ability to control."[89] The federal courts have held that the ability of a service provider to remove or block access to materials posted on its website or stored on its network is *not enough* to prove that the service provider had the "right and ability to control" the infringing activity.[90] Instead, the courts have required evidence of "something more" than the service provider's technical ability to remove or block infringing materials, which demonstrates the service provider's ability to exert "substantial influence on the activities of users."[91] For example, the federal district court in *Perfect 10, Inc. v. Cybernet Ventures, Inc.* found the requisite control where the service provider had established a monitoring program by which its webmasters received "detailed instructions regard[ing] issues of layout, appearance, and content."[92] The service provider also forbade certain types of content and refused access to users who failed to comply with its instructions. In addition, the appellate court in *Viacom International, Inc. v. YouTube, Inc.* suggested that "inducement of copyright infringement under *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, which "premises liability on purposeful, culpable expression and conduct," might also rise to the level of control under § 512(c)(1)(B).[93]

(...continued)

[85] *Id.* at 2070-71. (citations omitted).

[86] Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 35 (2d Cir. 2012).

[87] 718 F.3d 1006, 1023 (9th Cir. 2013).

[88] *Id.*

[89] 17 U.S.C. § 512(c)(1)(B).

[90] *Viacom*, 676 F.3d at 38.

[91] *Id.*

[92] 213 F. Supp. 2d 1146, 1173 (C.D. Cal. 2002).

[93] *Viacom*, 676 F.3d at 38.

c11173008

Recent Legislative Activities

Some copyright holders, particularly those who create and distribute music, television programs, and movies, have publicly expressed frustration with what they consider to be an "outdated" § 512 and would like Congress to require service providers to have more responsibility in preventing infringing activity.[94] In the 113th Congress, the House Judiciary Committee, Subcommittee on Courts, Intellectual Property, and the Internet, held a hearing on March 13, 2014, specifically regarding § 512 of the Copyright Act, in which it heard testimony from witnesses about the degree to which the safe harbor is, or is not, operating well.[95] House Judiciary Committee Chairman Goodlatte expressed concern about what he referred to as a "whack-a-mole game by copyright owners" who have to deal with repeated unauthorized postings of their content.[96] He explained the issue as follows:

> By most accounts, good faith service providers have acted expeditiously in responding to Section 512 notices by removing or disabling links to infringing content.
>
> However, copyright owners are increasingly facing a scenario that simply wasn't anticipated during the enactment of 512 – the need of copyright owners to send a voluminous amount of notices seeking removal of infringing content followed by the almost immediate reappearance of the same infringing content.

At the hearing, content owners argued that § 512, as currently written and interpreted by the courts, places too much burden on copyright owners to police infringing activity online,[97] whereas service providers urged Congress to keep the current DMCA framework unchanged and instead rely upon voluntary industry agreements and private industry solutions (such as content filtering systems) to address any infringement problems.[98]

Author Contact Information

Brian T. Yeh
Legislative Attorney
byeh@crs.loc.gov, 7-5182

[94] Nathan Pollard, *Panelists Debate Intentions of DMCA and Who Is Liable Under YouTube Decision,* BNA'S PATENT, TRADEMARK & COPYRIGHT JOURNAL, Aug. 5, 2011; Bill Donahue, *Google, Others Clash Over DMCA Safe Harbor,* Law360.com, Mar. 13, 2014.

[95] *Section 512 of Title 17: Hearing Before the House Judiciary Committee, Subcommittee on Courts, Intellectual Property, and the Internet,* 113th Cong., 2d Sess. (2014).

[96] *Id.* (opening remarks by Chairman Goodlatte).

[97] *Id.* (statement of Professor Sean M. O'Connor).

[98] *Id.* (statement of Katherine Oyama, Senior Copyright Policy Counsel, Google).

c11173008