

Do I Need a DMCA Agent?

By: Lawrence G. Walters, Esq.



I. Introduction:

Our law firm is often asked by clients, and potential clients, whether they should designate a DMCA Agent for their site, and how to go about doing so. While that is an important first question to ask, particularly for any site that contains material provided by third parties, it is only the beginning of a somewhat complicated analysis leading to a determination of whether a particular website can avail itself of the “safe harbor” protections against copyright infringement claims, as provided by federal law. Regardless of the geographic location of the website involved, compliance with U.S. DMCA safe harbor obligations is becoming essential for global online service providers.

II. The Development of the DMCA:

In 1998, in an attempt to curtail copyright infringement occurring via the Internet and harmonize international law, Congress passed the Digital Millennium Copyright Act (“DMCA”).¹ One of the most controversial and litigated elements of the DMCA is its “safe harbor” protection for “service providers.” Copyright holders tend to hate it, while website operators that allow posting of third party content view it as essential to survival of their business model. Given the recent wave of copyright infringement litigation being asserted against tube sites and other service providers, DMCA safe harbor is becoming an essential tool for website operators.

The DMCA’s safe harbor provisions allow certain online service providers (“OSPs”) who comply with specified statutory prerequisites to take advantage of significant limitations on monetary liability for copyright claims based on material posted by third party users on the service provider’s network. Simple enough, right? Post some legal-sounding takedown policies, file some forms, and you’re good to go. Not exactly... There are several important requirements, and even preconditions to those requirements, that an OSP must fulfill in order to even be considered for safe harbor protections. The following is a roadmap of sorts, designed to inform service providers of the hazards in navigating one of the Web’s most crucial and complicated pieces of legislation. However, this article is no substitute for legal advice, and if anything referenced in this post appears to affect your operation, a talk with your lawyer about DMCA issues is in order.

III. Who is a Service Provider?

Although a seemingly simple question, many providers of online services to end users on the Internet do not realize that the *type* of service they provide affects their obligations and potential protections under

⁷ 17 U.S.C. § 512(2010) *et seq.*

the DMCA. The DMCA defines a “service provider” as an entity offering transmission, routing, or providing 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, or, a provider of online services or network access, or the operator of facilities thereof.² Given its expansive definition, essentially any entity that provides end users with web space, bandwidth or access to the Internet could be considered a service provider under the DMCA. The types of business models covered by this definition range from ISP's, to online dating sites, to adult tube sites. The statute goes on to identify four categories of conduct that enable an OSP to determine which type of service provider they are under the DMCA:

1 – Transitory Communication Systems: Network services that simply provide transitory access to the Internet, this includes basically any broadband Internet provider (i.e. – AT&T and other DSL/cable/satellite Internet access providers);³

2 – Caching Systems: Network services still providing simple conduit access to the Internet, but that also may store or copy transmitted data temporarily;⁴

3 – Web Hosts: Online services that host content at the direction of a user (i.e. – traditional hosting websites or almost any website/network that contains content uploaded or generated by the network's users);⁵ or

4 – Information Location Tools: Search engines (i.e. – Google®)⁶.

Given the latest cyber litigation “target du jour”; user-generated content (“UGC”) websites, this article will only concentrate on potential limitation of liability for OSPs that host their users' files (i.e., #3 above). The legislative intent behind the file hosting safe harbor provision is to protect OSPs from liability based on the content posted by its users – whether in the form of online dating profiles or comments to a blog piece like this. For example, if UGC sites were responsible for each and every piece of infringing material uploaded by its users to the provider's network, such liability would likely bring much of today's Internet traffic to a screeching halt. OSPs that are required to monitor the content and/or conduct of their users would quickly find that the manpower necessary to accomplish that task would eat up any potential revenue to be generated, thus resulting in *de facto* censorship of an entire venue for online speech.

IV. Acquiring Potential Safe Harbor Protection?

² 17 U.S.C. § 512 (k)(1).

³ 17 U.S.C. § 512(a).

⁴ 17 U.S.C. § 512(b).

⁵ 17 U.S.C. § 512(c).

⁶ 17 U.S.C. § 512(d).

Notably, the safe harbor from liability is not a blanket grant of protection or immunity from suit. Even with full compliance with all aspects of DMCA safe harbor obligations, an OSP could still get sued by an aggressive plaintiff, and be forced to ‘prove up’ its safe harbor compliance regime. Importantly, an OSP may only qualify for the DMCA’s limitation on liability if it fulfills the threshold conditions of the statute by agreeing to do the following:

- 1 – Identify and Designate a DMCA Agent⁷
- 2 – Accommodate technical measures to protect copyrighted works⁸
- 3 – Adopt and Implement a Repeat Infringer Policy⁹

In order to facilitate the notification process required for safe harbor, OSPs must designate the name and contact information of an agent who will be responsible for receiving any infringement notices from copyright owners (i.e., a “DMCA Agent.”) Take down notices sent to the DMCA Agent must include specific elements, but they essentially must state that the OSP’s network contains content that is infringing upon the owners’ intellectual property rights and is therefore on the network illegally. Upon appointing the DMCA Agent, the OSP must file a notice of designation of agent with the U.S. Copyright Office, along with the required fee; effectually providing public notice of the relationship between the OSP and the agent.¹⁰ Unfortunately, this is a step that many OSPs tend to forgo, and the failure to properly designate the agency relationship with the Copyright Office may result in total loss of safe harbor protection. The information disclosed to the Copyright Office; i.e., name, address, phone number, and email address, must also be made readily available to the public through the OSP’s service or website.¹¹

The DMCA defines “standard technical measures,” referenced in #2 above, as attempts by intellectual property owners used to identify or protect their copyrighted works; for example, a watermark embedded on an image. An OSP accommodates, or does not interfere with, standard technical measures so long as it does not disable any such efforts by the copyright owner. Implementation of fingerprinting technology for identifying infringing videos or images may someday be considered a “standard technical measure” as such technology becomes more readily available and used by OSPs such as tube sites.

Another critical element must be met in order for an OSP to claim safe harbor: The OSP must adopt a policy that provides for terminating the accounts of users who repeatedly infringe on another’s copyright under “appropriate circumstances.” This is known in the industry as a “Repeat Infringer

⁷ 17 U.S.C. § 512(c)(2). Identification occurs by posting information about how to send DMCA notices to the agent on the website (i.e. – via a Notice and Takedown Policy), and Designation occurs by filing a Designation of Agent with the U.S. Copyright Office, and payment of the required fee. See United States Copyright Office website; available at: <http://www.copyright.gov/onlinesp/>.

⁸ 17 U.S.C. § 512(i)(1)(B).

⁹ 17 U.S.C. § 512(i)(1)(A).

¹⁰ See United States Copyright Office website; available at: <http://www.copyright.gov/onlinesp/>.

¹¹ 17 U.S.C. § 512(c)(2). This is accomplished through posting a proper Notice and Takedown Policy.

Policy” or “RIP.” The OSP must inform its customers of the RIP and “reasonably implement” it as well.¹² There are often two sources of confusion that correspond with the RIP requirement: Who is a “repeat infringer” and how do I “reasonably implement” a repeat infringer policy? Unfortunately for OSPs, the DMCA does not provide any guidance to resolve these ambiguities. For example, the statute does not specify whether the repetition requirement for a “repeat infringer” refers to the total number of works infringed, the number of times a single work has been infringed, or the number of times a particular user has been identified as an infringer. Nor does the statute discuss the time span within which the repeat infringements are to be calculated. Further, the DMCA does not identify particular actions that can be taken by an OSP to satisfy the statute’s requirement that it “reasonably implement” the RIP.

Ultimately, it is up to the OSP to decide exactly how it wishes to implement its RIP. Each business model may require its own type of RIP considerations, and there is no “magic number” of infringements that must result in termination of a user. Because of this lack of clarity in the statutory language, it has only been through OSPs being sued, and legal decisions being issued, that the public has gained some insight on the proper protocol in implementing an RIP. While no court has definitively described how a legally-compliant RIP should look, courts have discussed the importance of a consistent RIP to overall safe harbor protection.¹³

It should be noted that the law does not require OSPs to adopt an RIP, or to comply with any of the safe harbor provisions of the DMCA. OSPs can tolerate obvious repeat infringers, but they do so at their own peril. Compliance with DMCA safe harbor provisions is completely optional, but the benefits of compliance cannot be ignored, as a practical matter. Improper implementation of an RIP could result in the total loss of safe harbor protection, rendering OSPs completely vulnerable to traditional copyright claims based on direct, contributory and/or vicarious copyright infringement liability theories. Therefore, DMCA compliance comes down to a business decision – one that can be very important if the OSP is ever sued for copyright infringement based on UGC.

V. Loss of Safe Harbor Protection

Not only must an OSP fulfill the conditions referenced in the above section, but it must also meet the following constant obligations relating to its knowledge of specific infringing materials and its reaction to the knowledge of such materials. The DMCA specifically states that an OSP does not have a duty to monitor its network or actively seek out infringing activity in order to maintain its safe harbor status.

¹² 17 U.S.C. § 512(i)(1)(A).

¹³ See *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir. 2007); *IO Group, Inc. v. Veoh Networks, Inc.*, 586 F.Supp.2d 1132 (N.D. Cal. 2008)(The DMCA does not define “reasonably implement.” Nonetheless, the Ninth Circuit has held that a “service provider ‘implements’ a policy if it has a working notification system, a procedure for dealing with DMCA – compliant notifications, and it does not actively prevent copyright owners from collecting information needed to issue such notifications.” *CCBill*, 488 F.3d at 1109. “The statute permits service providers to implement a variety of procedures, but an implementation is reasonable if, under ‘appropriate circumstances,’ the service provider terminates users who repeatedly or blatantly infringe copyright.” *Id.*)

However, if the OSP is put on notice of infringement within its network, this then triggers the OSP's duty to act. An OSP may lose safe harbor protection if it:

- 1 – Has actual knowledge of the infringement;¹⁴ or,
- 2 – Is aware of facts or circumstances from which the infringing activity is apparent;¹⁵ and,
- 3 – Upon obtaining such knowledge or awareness, does not act expeditiously to remove, or disable access to, the infringing material.¹⁶

This means that safe harbor protection is available to OSPs only to the extent that the OSP has not been put on notice of particular infringing activity, or if it has, then it is obligated to remove the infringing content from its network. This also means that if certain "red flags" exist, suggesting rampant copyright infringement is apparent on the site, the OSP has a duty to act to take appropriate action to protect the copyright owners. Actual knowledge of alleged infringement is satisfied by receipt of a proper notice and takedown request from the copyright owner of the infringed upon material. The takedown notification must be in writing and must substantially contain the following information:

- 1 – The name, address, and electronic signature of the complaining party;¹⁷
- 2 – Identification of the infringing materials and their Internet location;¹⁸
- 3 – Identification of the copyrighted works that are being infringed upon;¹⁹
- 4 – A statement by the owner that it has a good faith belief that there is no legal basis for the use of the materials complained of;²⁰

¹⁴ 17 U.S.C. § 512(c)(1)(A)(i).

¹⁵ 17 U.S.C. § 512(c)(1)(A)(ii).

¹⁶ 17 U.S.C. § 512(c)(1)(C).

¹⁷ 17 U.S.C. § 512(c)(3)(A)(i).

¹⁸ 17 U.S.C. §§ 512(c)(3)(A)(ii-iii).

¹⁹ 17 U.S.C. § 512(c)(3)(A)(iv).

²⁰ 17 U.S.C. § 512(c)(3)(A)(v).

5 – A statement of the accuracy of the notice and, under penalty of perjury, that the complaining party is authorized to act on the behalf of the owner.²¹

So long as the DMCA notice is processed by the OSP, meaning, the notice is acknowledged by removal of the infringing material, it cannot be used as “actual notice” against the OSP in a subsequent secondary infringement claim.²²

DMCA Notices have become relatively commonplace in today’s online marketplace. Unfortunately, the recent trend has been to abuse the quick and easy content removal system put in place through the DMCA, by competitors seeking to get the upper hand by submitting false infringement reports about competing content. This sort of activity often occurs in the online escort site and online dating site industries. DMCA abuse can be punished by anyone suffering damages as a result, but often identifying the abuser can prove difficult, since the contact information provided in the Notice is often false. The OSP has no obligation to ensure that the contact information in DMCA Notice is valid or accurate – they are merely required to act when they receive a Notice containing the necessary elements.

Given the burden on the OSP to remove infringing content the moment it gains actual knowledge of infringement, or constructive knowledge through ‘red flags,’ the statute prevents such knowledge to be used against the OSP so long as it discharges its removal obligations. In other words, the DMCA allows OSPs to remain within the realm of safe harbor protection, even after acquiring knowledge (whether actual *or* apparent) of infringing content, so long as the OSP “acts expeditiously to remove, or disable access to, the material.”²³

VI. Consequences of Safe Harbor Loss

The primary consequence of losing DMCA safe harbor protection is exposure to monetary damages (i.e. – “all damages, costs, attorneys’ fees, and any other form of monetary payment,”) however it is within a court’s discretion to issue injunctive relief against them as well. Such injunctions may mandate any actions that the court considers necessary to prevent subsequent infringement of the material in question.²⁴ Loss of safe harbor protection does not mean that the OSP is automatically responsible for infringing content posted by third parties; it simply means that the OSP cannot assert the safe harbor defense. A copyright claimant would still need to prove the standard elements of copyright infringement before the OSP could be held liable.

²¹ 17 U.S.C. § 512(c)(3)(A)(vi).

²² 17 U.S.C. § 512(c)(1)(A)(iii).

²³ *Id.*

²⁴ 17 U.S.C. § 512(j)(1)(iii).

In the event that an OSP attempts half-hearted DMCA compliance, whether intentional or not, it may not be able to rely on the statute to come to its rescue if it is ultimately sued for copyright infringement based on infringing UGC on its network. Thus, merely posting the name of a person who has agreed to serve as your DMCA agent on your 'Contact Us' page does not grant an OSP any safe harbor protection. Yet, many OSP's – particularly those located overseas who are not conversant in U.S. legal requirements – tend to assume that listing a DMCA agent constitutes a 'magic shield' that will protect them from any U.S. claimants seeking to impose monetary liability for third party generated content.²⁵ As demonstrated above, full DMCA safe harbor protection is much more complicated to achieve.

VII. Conclusion

Although acquiring DMCA safe harbor can be a burden, any compliance regime should be developed in consultation with legal counsel. The benefits of proper DMCA compliance are substantial. Few federal statutes provide a complete release of liability for a category of intellectual property infringement, and thus all OSPs that allow any UGC should strongly consider developing strict DMCA safe harbor compliance policies. DMCA safe harbor is one of the greatest shields provided to OSPs, but like most armor, if it not properly applied, it can turn the wearer into nothing more than a target.

*Lawrence G. Walters, Esq., heads up [Walters Law Group](#), a law firm which represents clients involved in all facets of the adult industry. The firm handles First Amendment cases nationwide, and has been involved in Free Speech litigation at all levels, including the United States Supreme Court. All statements made in the above article are intended for general informational purposes only and should not be considered legal advice. Please consult your own attorney on specific legal matters. You can reach Lawrence Walters at larry@firstamendment.com. More information about **Walters Law Group** can be found at www.FirstAmendment.com.*

²⁵ Not only is this factually inaccurate, but as discussed above, the DMCA has no applicability to certain claims like trademark or cybersquatting claims, which could still be asserted against OSPs that are in full compliance with the DMCA.