STOEL RIVES LLP
ATTORNEYS AT LAW

BEST PRACTICES FOR WIRELESS ACCESS PROVIDERS TO AVOID COPYRIGHT INFRINGEMENT LIABILITY

By Matti Neustadt Storie

DIGITAL COPYRIGHT BACKGROUND **2**

1. Safe Harbors **3**
1.1. Internet Service Providers 3
1.1.1. Conduit Safe Harbor (§512(a)) 4
1.1.2. **Systems Caching Safe Harbor (§512(b))** 5
1.1.3. **Material Stored at User Discretion Safe Harbor (§512(c))** 6
1.1.4. Information Location Tools Safe Harbor (§512(d)) 7
1.2. Safe Harbors as Incentives 8

2. Termination Policy Best Practice **8**
2.1. Infringement Notice Requirements 9
2.2. Counternotice 10

3. Implementation of Policy Best Practice **11**
3.1. Notice of Policy Best Practice 11
3.2. Accommodating Technological Measures of Protection 12

4. Indirect Infringement Liability Standard **12**

5. Subpoenas **13**

WIRELESS ACCESS PROVIDERS **14**

CONCLUSION **15**

APPENDIX A: EXAMPLE NOTIFICATIONS OF DMCA POLICY **17**

Comcast.net (http://www.comcast.net/terms/use.jsp, last checked 8/28/07) **17**

Google.com (http://www.google.com/dmca.html, last checked 08/28/07) **18**

Digital Copyright Background

The Copyright Act (17 USC et. seq.) provides protection from unlawful reproduction, distribution, display, production of derivate works, and public performance of a work. All copyrighted works fixed in a tangible medium of expression gain protection under this law, regardless of the medium in which the work is fixed. This includes works fixed in digital form, such as information stored in a computers hard drive or memory.

The advent of digital media and the internet has challenged traditional copyright law. The broad protection against any copying was difficult to reconcile with the way computers worked, providing copyright infringement even when a computer user had a license for the work. An early case, *MAI Systems Corp. v. Peak Computer, Inc.*[1], held that copying in a computer's RAM constituted an infringing copy even though the computer automatically made the copy and the copy existed only for a short time in order to allow a technician to service a computer through remote access. The Digital Millennium Copyright Act (DMCA) of 1998, which created an exemption for copies made for maintenance or repair, later overruled the specific circumstances in MAI but the ruling in *MAI* still proved difficult to work with.

Complicating matters further was the advent of the internet. Transmissions over the internet require servers and network routers to create multiple copies of materials in order to transmit content from one user to another. These copies, viewed under *MAI*, are infringing copies even if the users who were transferring the copies over the internet both had valid permissions to make copies for their own use because the network server and router owners lacked that permission.

Traditional copyright notions of secondary liability through contributory infringement or vicarious liability made matters even more difficult for the network providers. Contributory infringement is when a third party (not the direct infringer) has knowledge of the infringement and induces, causes or materially contributes to the infringement, and results in liability for the infringement. Vicarious liability is liability resulting from holding a financial interest in the infringing activity and the right and ability to control the infringing activity. Intent or knowledge is not required for vicarious liability, nor is actual control so long as the right or ability to control

[1] 991 F.2d 511 (9th Cir. 1993)

is present. Vicarious liability holds the greatest risks for online service providers because it could be liable for the infringing activities of any user of the provider who infringed.

Congress enacted Title II of the Digital Millennium Copyright Act (DMCA) in an effort to limit liability of network service providers. It balanced the limited liability with incentives for the providers to take action against known copyright infringement. This memo outlines the key issues surrounding limited liability under the DMCA and steps a provider of online services can take to reduce its own liability.

1. Safe Harbors

One of the best ways an online service provider can avoid liability for copyright infringement is to qualify as an Internet Service Provider (ISP) under one or more safe harbors provided in the DMCA. Neither Congress nor the courts defined what is and is not an ISP under the DMCA. The statute provides four separate safe harbors, however, which helps classify various types of ISPs, but is not limited. Telecommunications companies who typically provide internet service to consumers commonly use the "transitory" or "conduit" safe harbor. The "caching" safe harbor is commonly used by server owners who facilitate consumer-to-consumer transactions. Bulletin board systems or website operators commonly use the "user discretion" or "BBS" safe harbor. Search engine providers commonly use the "information location tools" safe harbor.[2] None of the safe harbors are limited to the type of ISP which typically use the safe harbor, and the definition for the statutes is generally interpreted more broadly than the common language definition of an ISP.

1.1. Internet Service Providers

The DMCA safe harbor statute contains two definitions of ISP, applicable for the four different safe harbors. Many consider only the telecommunication companies that provide consumers with direct access to the internet to be an "internet service providers". The DMCA statute, however, broadens this definition is considerably, and has allowed online services such as bulletin board services, search engines, and online marketplaces to be classified as ISPs.

[2] 17 USC 512(a),(b), (c)(1), and (d), respectively.

The first definition for an ISP is 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.[3] This definition is the most restrictive definition and only applies to entities seeking protection from liability under the "transitory digital network communications" safe harbor.[4] An ISP under this definition includes any provider who plays solely the role of a "conduit" for the communications only when the communications pass through the system of the ISP.[5] Entities seeking safe harbor under the caching, user discretion or information location tools may take advantage of a broader definition. However, even under the more restrictive definition of ISP, bulletin boards and companies such as AOL have found safe harbor from copyright infringement claims because of the nature of their services.[6]

The §512(b)-(d) definition of ISP is a more general requirement for the entity to provide an online service or network access, or operate facilities for that purpose. However, these section come as an "incentive" for having in place notice and takedown practices which protect copyright owners more rigorously than the safe harbors under §512(a).

1.1.1. Conduit Safe Harbor (§512(a))

ISPs providing the intermediate or transient storage of material in the course of transmitting, routing or providing connections are exempt from monetary damages related to vicarious liability[7]. The protection for transient storage further protects ISPs who not only route communications through their systems, but may also need to temporarily store information on their servers or equipment, which would normally be an infringing activity under *MAI*.

The transitory safe harbor is only available when material that passes through an ISP's network at the requests of users interacting with each other. The material must pass through the network, be done *at the users' requests*, and cannot be kept in the network longer than necessary.

[3] 17 USC §512(k)

[4] 17 USC §512(k)(1)(B)

[5] *A&M Records, Inc. v. Napster, Inc.*, 114 F.Supp.2d 896 (N.D. Cal. 2000).

[6] See generally, *Ellison v. Robertson*, 189 F.Supp.2d 1051 (C.D. Cal 2002)

[7] All safe harbors in the DMCA protect only from *monetary* relief. Relief in the form of an injunction is possible under the act, but rarely seen when the defendant successfully invokes the safe harbors.

In *A&M Records, Inc. v. Napster, Inc.,* Napster attempted to but did not qualify for the limited liability under §512(a) because it did not serve merely as a conduit through which communications passed. In fact, it allowed users to pass information directly from one computer to another without ever going through Napster's servers or network paths.

Additionally, to qualify under this section, an ISP must not store material on its network equipment and servers any longer than necessary to allow the material to be passed from one user to another. ISPs seeking safe harbor are limited to "transient" storage. Unfortunately, the statute does not provide guidance as to what period constitutes "transient" when applied to data storage. Infringing copies held for 14 days on servers of AOL were considered transient because they were not stored for longer than reasonably necessary for their routing, and dicta is other cases provide for a transient period of up to 20 days.[8] Also considered transitory were those entities that provided the service of age verification for adult-only websites so long as they were not stored for a time longer than reasonably necessary.[9]

1.1.2. **Systems Caching Safe Harbor (§512(b))**

System caching is another type of temporary data storage used to facilitate internet communications and make them more efficient. Caching is similar to transitory storage in that the material is temporarily stored in ISP servers. Caching is distinguished from transient conduit storage because it is an automatic process used for frequently accessed material. A user will request the information first, causing it to be stored in the system's cache by means of a copy. The difference between caching and transitory storage is whether the material is stored on the servers by the users' request (transitory storage) or through an automated process of the ISP (caching).

An ISP can store cached information for a temporary period. In *Fields v. Google,* this temporary period was seen to be the same as the allowable transitory period for §512(a). While still not definitively set, a period of 20 days was held to be temporary. The material must also be stored through an automatic technical process, including automated software, for the purpose of

[8] See generally: *Ellison v. Robertson*, 189 F.Supp.2d 1051 (C.D. Cal 2002), *Field v. Google, Inc.*, 412 F. Supp.2d 1106 (D.Nev. 2006).

[9] *Perfect 10, Inc. v. CCBILL*, 340 F.Supp.2d 1077 (C.D. Cal. 2004), *affirmed in part, remanded in part* at 481 F.3d 751 (9th Cir. 2007).

making the material available to users of the system who request the material. This is precisely what is done when an ISP sets up technical procedures that allow users to efficiently reach frequently accessed information over the web through automated caching. Caching can be done on traditional ISP servers, intermediate memory (such as search engines servers and network routers), and end user personal computers. Because the definition of ISP under §512(b) is more relaxed than the definition under §512(a), many providers of any type of online service may be considered an ISP which can take safe harbor from copyright infringement under this provision. However, safe harbor for caching is available only if the notice and takedown procedures of §512(c) are met.

1.1.3. **Material Stored at User Discretion Safe Harbor (§512(c))**

The limitation of liability for those ISPs who allow information stored at the request and discretion of the user most frequently used to protect those ISPs hosting web pages created by third parties. Information residing on an ISP's system or network *at the discretion of the ISP and not at the discretion of a user* does not fall within the limits of liability under this section. A provider of online services storing data on its own servers at its own discretion would not qualify as an ISP under this section and could not take safe harbor even with effective termination policies in place.

An ISP may not take advantage of the safe harbor in §512(c), however, if it meets the standards of vicarious liability – that is, it has knowledge of the infringing activity, receives a financial benefit because of the infringing activity. The DMCA, however, makes the knowledge requirement more difficult to meet than it is in traditional copyright law. An ISP has the right to receive notice that substantially meets the statutory requirements, and cannot have constructive knowledge based on a defective notice. The notice must meet all the requirements of §512(c)(3) (more below). While this section may impute constructive knowledge of infringement on an ISP, a defective notice will not be sufficient to provide constructive knowledge. Once an ISP has knowledge of infringement, it faces liability only if it fails to take down the infringing material or restrict access to the infringing party.[10]

[10] 17 USC §512(c)(1)(A) - (C).

Courts have also narrowly construed the meaning of "financial benefit" when considering the ability of an ISP to take the safe harbor. It is not sufficient for the ISP simply to be a commercial activity; it must also receive a financial benefit specifically caused by the infringing activity, such as customers who seek the ISP out because it allows for copyright infringement. The test for a receipt of direct financial benefit requires that the infringing activity must "act as a draw" to the site[11], but is considered regardless of whether the financial benefit is substantial.[12] Additionally, vicarious liability does not require a significant financial benefit. The financial benefits test is only relevant to those ISPs which have a "right and ability to control" the infringing activity.[13] Having the ability to remove access or delete content is not sufficient to show this control – there must be something more, such as a proactive policy to search for and remove infringing content.[14]

1.1.4. Information Location Tools Safe Harbor (§512(d))

Online service providers who provide information location tools, such as directories, search engines, and sites with hyperlinks, may be considered an ISP with limited liability under §512(d). In *Perfect 10, Inc. v. CCBill*, LLC, the court determinatively stated the ISP safe harbor in §512(d) is not limited to those like Yahoo! or Google who provide links to millions of sites to whom they have no relation.[15] The district court in *A&M Records, Inc. v. Napster* held that Napster included protected internet search functions such as lists of files each user offered, a search function permitting users to look for a particular song or artist and a search function permitting users to look for log-in names of other users on the Napster system.[16] (the court did not determine if Napster should be allowed the safe harbor under §512(d) because it was not pled).

As with other storage-based ISPs (§512(b) & (c)), ISPs seeking safe harbor as an information location tool must meet the incentive requirements under §512(c). Appropriate

[11] *A&M Records, Inc. v. Napster, Inc.*, 114 F.Supp.2d at 921
[12] *Ellison v. Robertson*, 357 F.3d 1072, 1079 (9th Cir. 2004)
[13] 17 USC §512(c)(1)(B)
[14] See the *Hendrickson* cases, generally.
[15] *Perfect 10, Inc. v. CCBill*, 340 F.Supp.2d at 1098
[16] *A&M Records, Inc v. Napster*, 54 USPQ2d 1746 (N.D. Cal. 2000).

notice and takedown procedures and lack of vicarious liability are similarly necessary for information location provider ISPs.

1.2. Safe Harbors as Incentives

The safe harbors are possible only as incentives for reducing overall copyright infringement. Additional requirements are necessary, beyond being qualified as an ISP, in order to eliminate liability. A qualifying ISP must adopt a policy of terminating repeat infringers, implement that policy in a reasonable manner, and inform its users of the policy.[17] Additionally, the ISP cannot gain direct financial benefit directly related to the infringing activity while having the right and ability to control such activity.[18] An ISP must also not induce or materially contribute to copyright infringement.

As previously noted, incentives are different based on which safe harbor is sought by the ISP. ISPs seeking safe harbor as a mere conduit have fewer requirements to get the incentive, but face a stricter definition of ISP. ISPs which seeking safe harbor as something other than a mere conduit have an additional requirement in order to avoid liability, the "notice and take-down" provision. The notice and take-down provision is the requirement under §512(c)(3), which provides an ISP must expeditiously remove or disable access to infringing notice after proper notification is given. The notice and take-down provision is an additional requirement only for those ISPs which store infringing material on its own servers, and not those ISPs who act as a mere conduit for the data.

2. Termination Policy Best Practice

An ISP that seeks safe harbor for third party copyright infringement must adopt a policy that seeks to terminate a repeat infringer. A qualifying policy must include a working notification system and a procedure for dealing with DMCA-compliant notifications. Neither the policy nor its implementation can actively prevent copyright owners from notifying the ISP or collecting information necessary to notify the ISP of infringement.[19] The focus is on terminating

[17] 17 USC §512(i)
[18] 17 USC §512(c)(1)(B)
[19] 17 USC §512(i)(1)

infringing *users*, and not repeating infringing *content*.[20] Repeat postings or storage of infringing content, provided by different users, are not a violation of a qualifying policy. A repeat infringer also must infringe at least twice in order to be considered a repeat offender.[21]

A termination policy is only required to be reasonable, and not perfect in preventing copyright infringement. A policy is reasonable if it makes a record of most users in order to identify repeat offenders. An ISP must be able to identify repeat offenders, notify them of the removal of any suspected infringing materials or the disabling of a user's account access. The policy must also state it will remove infringing material and provide a communication path for counternotification.

A conduit ISP is not required to have in place these notice and takedown policies because it does not store material and, therefore, cannot be required to remove it. A conduit ISP that wishes to be extra vigilant in protecting copyright owners' rights may also be wary of implementing a policy that disables access to a particular user because of copyright infringement because of the administrative costs involved. Viacom has sent over 160,000 take down notices to Google related to its content on YouTube[22] and pays an outsourcing company more than $100,000 per month to track allegedly infringing content and send takedown notices.[23] The costs associated with responding to a high number of requests may be more than an ISP may want to undertake.

2.1. Infringement Notice Requirements

The termination policy is not required to remove content or disable access based on any request; only a notification of infringement which is compliant with §512(c)(3) will trigger the requirement. A compliant notice must be a written and signed communication to ISP's designated agent. It must identify the complaining party, the copyrighted work, and the material claimed to be infringing with particularity "reasonable sufficient to permit the service provider to

[20] *Perfect 10 v. CCBILL*, 340 F.Supp.2d at 1088 (emphasis not in original)
[21] Id. at Footnote 12
[22] *Viacom Nets, Releases Another Fair Use Dolphin*, http://www.eff.org/deeplinks/archives/005327.php (last checked 08/30/07)
[23] Kevin Delany, *YouTube Magic:Now You See It, Now You Don't. Hired Eyes Make Sure That Copyrighted Videos Are Yanked From the Web*, The Wall Street Journal (August 8, 2007, A1)

locate the material".[24] It must include two statements similar to an affidavit. The statement "the complaining party has 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" must be include. Also a statement that the "information in the notification is accurate, and under the penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed" must be included.[25] Failure to provide the statement of good faith belief and affidavit of authority is not reasonable compliance with the DMCA notification procedures and does not provide notice.[26] However, partial notice, which sufficiently identifies the complaining party and infringing material but is missing the statements, requires the ISP to follow up with the complaining party in order to get a compliant notice. The ISP must act "expeditiously" to remove the allegedly infringing material once compliant notice is given.[27]

Once compliant notice is received, the ISP is deemed to have notice of infringement and is subject to liability. The ISP must then contact the user who is the alleged infringer in the notice and allow the user to file a counternotice.

2.2. Counternotice

Termination of a user account or removal of a user's material because of a DMCA compliant notice may be premature if the allegedly infringing material qualifies as fair use, or some other defense that protects the user's right to copy the material. Depending on the nature of the material, removal of the material or the user's access may provoke questions of interference with free speech rights. An ISP should take additional steps with the accused infringer to ensure liability remains limited under the safe harbors.

In addition to notifying the accused infringer of the action taken (i.e. taking the material down or disabling access), the ISP must allow the user to file a compliant counternotice stating he or she has a right to the allegedly infringing material. The counternotification must meet the same requirements as the original notification in order to be effective. Once the ISP receives a compliant counternotification, the ISP must notify the party who filed the takedown notice. If

[24] *Hendrickson v. Ebay, Inc.*, 165 F. Supp.2d 1082 (C.D. Cal. 2000)
[25] 17 USC §512(c)(3)
[26] See generally, *Hendrickson v. Ebay, Inc.*, *Perfect 10 v. CCBILL*
[27] 17 USC §512(c)(1)(A)(iii)

the copyright holder or his agent does not file suit within 14 days of notice of the counternotice, the ISP must restore the material and access to the accused user. The ISP will not be liable for reinstating the allegedly infringing material or allowing access to the alleged infringer if it takes these counternotification steps.

3. Implementation of Policy Best Practice

Congress requires a reasonable implementation of a termination policy rather than perfect implementation.[28] An ISP “implements” a policy if it has a working notification system, an operating procedure for dealing with DMCA-compliant notifications, and if it does not actively prevent copyright owners form collecting information needed to issue such notifications.[29] The implementation is reasonable if, under “appropriate circumstances”, ISPs terminate users who repeatedly or blatantly infringe copyrights.[30] Reasonable implementation does not require an ISP to police proactively its users for evidence of repeat infringement.[31]

Case law is conflicted over the level of tracking required to be part of a reasonable implementation of a termination policy. Perfect records of DMCA-compliant notices are not required. In *Perfect 10 v. CCBill*, the defendant kept track of DMCA-compliant notices and repeat offenders, although the tracking list did not include every webmaster name. The court held the implementation to be reasonable. In both *In re Aimster Copyright Litigation* and *Ellison v. Robertson*, the implementation was not reasonable. Aimster encrypted its user information to the point where no one could ascertain which users where transferring which files. AOL (the ISP in the *Ellison* case) changed the email address to report alleged infringement without notifying the copyright office or any of its customers. In many cases, implementation is reasonable even if the implementation ignores infringement notices that do not substantially comply with the DMCA guidelines.

3.1. Notice of Policy Best Practice

[28] *Perfect 10 v. CCBILL*, 481 F.Supp.3d 751 at 758
[29] *Id.*
[30] *Id.* at 759
[31] I. at 769

The DMCA requires that ISPs notify users of the termination policy for repeat offenders. Most ISPs do this in their Terms and Conditions for Use agreements or other agreement a user is required to accept before using the ISP services. The ISP also notifies the Copyright Office of the agent who designated to receive infringement notices.

No case law exists as to what is and is not sufficient notice to users under this requirement. It is suggested to include, at a minimum:

(1) A statement that the ISP complies with the DMCA;
(2) An email or postal service address of a designated agent who is responsible for receiving infringement notices;
(3) The procedure for notifying of infringement and countering such notice; and
(4) A statement indicating the ISP will seek safe harbor under the DMCA for third party copyright infringement.

Samples of various conduit-type ISPs are available as Appendix A.

3.2. Accommodating Technological Measures of Protection

The last requirement of the DMCA in order for an ISP to take safe harbor under §512 is the requirement for an ISP to accommodate technical measures of protection in copyrighted works[32]. While this covers standard measures such as password protection, it may also covers more advanced forms of technical protection. An ISP should not disable access or prevent files containing Digital Rights Management (DRM) software or code, which is code specifically designed to protect intellectual property rights and prevent unauthorized copying. Interfering with DRM has consequences beyond loss of Safe Harbors, a separate section of the DMCA prohibits circumventing DRM.[33]

4. Indirect Infringement Liability Standard

Despite the safe harbors, an ISP may be liable for copyright infringement through claims other than vicarious liability. The DMCA Safe Harbors protect against vicarious liability in limited circumstances, but do not protect an ISP from contributory infringement. An ISP will

[32] 17 USC §512(i)(1)(B)
[33] 17 USC §1201

face liability as a contributory infringer when a user directly infringes on a copyrighted work, the ISP had knowledge of the infringement, and induced, caused, or materially contributed to the infringing activity.

The level of contribution which is considered “material” in traditional copyright law was often considered under the “swap meet” test provided under *Fonovisa v. Cherry Auction, Inc.* The court in *Fonovisa* found contributory infringement when the defendant provided the site and facilities for known infringement and benefited financially from the enhanced attractiveness of the infringing activities[34]. ISPs that enjoy protection under the Safe Harbors for simply providing the computerized equivalent of a “site” or “facilities” can still be liable if it actively participates or induces the infringement. When an ISP does induce or materially contribute to infringement, actual knowledge of the third party’s infringement is not necessary to provide liability. The U.S. Supreme Court stated “one who distributes a device with the object of promoting its use to infringe copyright, as shown by the clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties”.[35] An ISP cannot take safe harbor and avoid liability simply by willfully closing its eyes to infringement that it promotes, enables and provides benefit.

5. Subpoenas

One of the greatest difficulties facing copyright holders in stopping online infringing activity is the ability to identify the primary infringer. Plaintiffs do not sue ISPs only because ISPs tend to have the proverbial “deep pockets”; they also do so because the primary infringers can be very difficult to identify. Most infringers identify themselves online only by a screen handle, such as “jdoe888”. To promote enforcement of copyrights against actual infringers, the DMCA provides for the ability to subpoena an ISP for identification of an alleged infringer.[36] The DMCA requires the clerk to issue a subpoena when the request for such subpoena includes a compliant request for subpoena. A compliant request identifies the copyrighted works and the infringing material with enough particularity for the ISP to identify and locate the material, and includes the proposed subpoena and a sworn declaration that the purpose of the subpoena is to

[34] Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996)
[35] Metro-Goldwyn-Mayer Studios, Inc v. Grokster, 545 U.S. 913 (2005)
[36] 17 USC §512(h)

identify the alleged infringer and protect copyright rights.[37] When the request properly contains this information, the clerk has no discretion and must grant the subpoena.

A copyright holder's ability to subpoena an ISP for the identity of its users has been limited by current case law. Both the DC Circuit and the 8th Circuit have ruled directly on point, holding a subpoena may only be issued to an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity. ISPs that operate only as a conduit and do not store material on its own servers are not subject to the §512(h) subpoena powers.[38] The key to notice under the subpoena power is that the notice requirements are the §512(c)(3) requirements, commonly called the "notice and take-down" requirement. This notice and take-down provision is a requirement for a subpoena, the courts have reasoned, so a conduit ISP can not be subpoenaed because they are not subject to the notice and take-down provision.

Wireless Access Providers

A wireless access provider (WAP) is an entity that provides internet connection through a wireless local area network (LAN). WAPs are the source of local area "hot spots", venues that provide internet access to users with appropriate computers. These hot spots are usually found at local restaurants, coffee shops, airports and hotels and may be either free or pay-per-service. A WAP does not generally host user websites, host their own website, or provide end-user software to its users.

Under the DMCA, a WAP is a conduit ISP because it offers transmission, routing and provision for connections for digital online communications, between points specified by a user and of material of the user's choosing, without modification. This is the definition of an ISP provided by §512(a), applicable to the safe harbor for transient storage of conduit ISPs. Classifying a WAP as a conduit ISP, however, is based on the statutory definition and may be jeopardized if the WAP were to provide its own content or transmit material of its own choosing rather than the user's choosing. Strict compliance with the definition of a conduit ISP is

[37] 17 USC §512(h)(2)(A)-(C)

[38] See generally, *Recording Industry Association of America v. Verizon Internet Services, Inc.*, 351 F.3d 1229 (D.C. Cir. 2003), and *In re Charter Communications, Inc.*, 393 F.3d 771 (8th Cir. 2005)

necessary to ensure limited liability without the need for notice and takedown provisions. An ISP may also be able to quash a subpoena seeking its users' personal information if it is in strict compliance with the conduit ISP definition.

Failure to set up a WAP to be in strict compliance with the statutory definition of a conduit ISP does not guarantee liability for vicarious infringement. A WAP may still qualify as an ISP under one of the other safe harbors. However, the other safe harbors carry the additional requirements of the notice and takedown policy outlined above, and further policies and procedures should be implemented in order to gain safe harbor under one of the other definitions of an ISP.

Conclusion

Providers of online access and services have many opportunities to avoid liability for third party copyright infringement. These opportunities are balanced with the need for the ISPs to work with copyright owners to enforce copyright protections. An ISP should take the necessary steps to make full use of the opportunities for limited liability.

Regardless of the type of service an ISP provides, it put in place a DMCA policy stating its goal is to comply with the DMCA and implement reasonable procedures allowing it to do so. For non-conduit ISPs, the DMCA policy must state that repeat copyright infringers will loose access and the infringing material removed. The ISP should designate and train an agent to receive DMCA compliant notifications and react to those notices to notify the alleged infringer and follow up with the complainant as necessary.

An ISP seeking protection as a mere conduit should as little data as possible on its servers. If data must be stored on the conduit ISP's servers, it should not be stored any longer than necessary (a "transient" period) to allow the data to travel from point A to point B, and should be stored automatically. If the ISP is seeking protection as any other type of service provider, the ISP should have in place a notice and takedown procedure for alleged infringing material. A non-conduit ISP should also have a system in place to identify and track repeat offenders based on notifications. The ISP does not have the responsibility to monitor for infringement, only to track DMCA-compliant notice and recognize when those notices identify a repeat infringer.

Most importantly, an online service provider must not engage in business practices that promote, solicit or induce copyright infringement. Courts look suspiciously on business models that encourage users to share unlicensed copyrighted works without the copyright holders' permissions. Liability for this type of activity will not be limited and may include monetary damages, injunctive relief and punitive damages. It is unlikely that a business model based on revenue generated solely or primarily on copyright infringement will be able to take advantage of any of the safe harbors provided by the DMCA.

Appendix A: Example Notifications of DMCA policy

Comcast.net (http://www.comcast.net/terms/use.jsp, last checked 8/28/07)

Copyright Infringement

Comcast is committed to complying with U.S. copyright and related laws, and requires all customers and users of the Service to comply with these laws. Accordingly, you may not store any material or content on, or disseminate any material or content over, the Service (or any part of the Service) in any manner that constitutes an infringement of third party intellectual property rights, including rights granted by U.S. copyright law. Owners of copyrighted works who believe that their rights under U.S. copyright law have been infringed may take advantage of certain provisions of the Digital Millennium Copyright Act of 1998 (the "DMCA") to report alleged infringements. It is Comcast's policy in accordance with the DMCA and other applicable laws to reserve the right to terminate the Service provided to any customer or user who is either found to infringe third party copyright or other intellectual property rights, including repeat infringers, or who Comcast believes in its sole discretion is infringing these rights. Comcast may terminate the Service at any time with or without notice for any affected customer or user.

Copyright owners may report alleged infringements of their works that are stored on the Service or the Personal Web Features by sending Comcast's authorized agent a notification of claimed infringement that satisfies the requirements of the DMCA. Upon Comcast's receipt of a satisfactory notice of claimed infringement for these works, Comcast will respond expeditiously to either directly or indirectly (i) remove the allegedly infringing work(s) stored on the Service or the Personal Web Features or (ii) disable access to the work(s). Comcast will also notify the affected customer or user of the Service of the removal or disabling of access to the work(s). If the affected customer or user believes in good faith that the allegedly infringing works have been removed or blocked by mistake or misidentification, then that person may send a counter notification to Comcast. Upon Comcast's receipt of a counter notification that satisfies the requirements of DMCA, Comcast will provide a copy of the counter notification to the person who sent the original notification of claimed infringement and will follow the DMCA's procedures with respect to a received counter notification. In all events, you expressly agree that Comcast will not be a party to any disputes or lawsuits regarding alleged copyright infringement.

Copyright owners may send Comcast a notification of claimed infringement to report alleged infringements of their works to:

G. Lipscomb and C. Padgett
Comcast Cable Communications, LLC
650 Centerton Road
Moorestown, NJ 08057 U.S.A.
Phone: (856) 317-7272
Fax: (856) 317-7319
E-mail: dmca@comcast.net

Copyright owners may view and print a notification of claimed infringement form in HTML format. Complete the form and return it to Comcast. Comcast doesn't require that you use this form, and copyright owners may use their own notification of claimed infringement form that satisfies the requirements of Section 512(c)(3) of the U.S. Copyright Act. Under the DMCA anyone who knowingly makes misrepresentations regarding alleged copyright infringement may be liable to Comcast, the alleged infringer, and the affected copyright owner for any damages incurred in connection with the removal, blocking, or replacement of allegedly infringing material.

If a notification of claimed infringement has been filed against you, you can file a counter notification with Comcast's designated agent using the contact information shown above. All counter notifications must satisfy the requirements of Section 512(g)(3) of the U.S. Copyright Act.

Google.com (http://www.google.com/dmca.html, last checked 08/28/07)

It is our policy to respond to clear notices of alleged copyright infringement. This page describes the information that should be present in these notices. It is designed to make submitting notices of alleged infringement to Google as straightforward as possible while reducing the number of notices that we receive that are fraudulent or difficult to understand or verify. The form of notice specified below is consistent with the form suggested by the United States Digital Millennium Copyright Act (the text of which can be found at the U.S. Copyright Office Web Site, http://www.copyright.gov) but we will respond to notices of this form from other jurisdictions as well.

Regardless of whether we may be liable for such infringement under local country law or United States law, our response to these notices may include removing or disabling access to material claimed to be the subject of infringing activity and/or terminating subscribers. If we remove or disable access in response to such a notice, we will make a good-faith attempt to contact the owner or administrator of the affected site or content so that they may make a counter notification. We may also document notices of alleged infringement on which we act. Please note that in addition to being forwarded to the person who provided the allegedly infringing content, a copy of this legal notice may be sent to a third-party partner for publication and annotation. As such, your letter (with your personal information removed) may be forwarded to Chilling Effects (http://www.chillingeffects.org) for publication. You can see an example of such a publication at http://www.chillingeffects.org/dmca512/notice.cgi?NoticeID=861.

Infringement notification
Counter notification
Infringement Notification for Web Search and all other products

To file a notice of infringement with us, you must provide a written communication (by fax or regular mail -- not by email, except by prior agreement) that sets forth the items specified below. Please note that you will be liable for damages (including costs and attorneys' fees) if you materially misrepresent that a product or activity is infringing your copyrights. Indeed, in a recent case (please see http://www.onlinepolicy.org/action/legpolicy/opg_v_diebold/ for more information), a company that sent an infringement notification seeking removal of online materials that were protected by the fair use doctrine was ordered to pay such costs and attorneys fees. The company agreed to pay over $100,000. Accordingly, if you are not sure whether material available online infringes your copyright, we suggest that you first contact an attorney.

To expedite our ability to process your request, please use the following format (including section numbers):

1. Identify in sufficient detail the copyrighted work that you believe has been infringed upon (for example, "The copyrighted work at issue is the text that appears on http://www.legal.com/legal_page.html") or other information sufficient to specify the copyrighted work being infringed (for example, "The copyrighted work at issue is the “Touch Not This Cat” by Dudley Smith, published by Smith Publishing, ISBN #0123456789").

2. Identify the material that you claim is infringing the copyrighted work listed in item #1 above.

FOR WEB SEARCH, YOU MUST IDENTIFY EACH SEARCH RESULT THAT DIRECTLY LINKS TO A WEB PAGE THAT ALLEGEDLY CONTAINS INFRINGING MATERIAL. This requires you to provide (a) the search query that you used, and (b) the URL for each allegedly infringing search result.

For example, suppose (hypothetically) that you conducted a search on google.com using the query "google", and found that the third and fourth results directly link to a web page that you believe infringes the copyrighted text you identified in item #1 above. In this case, you would provide the following information:

Search Query: google
Infringing Web Pages: www.infringingwebsite.com
directory.infringingwebsite.com

If you are sending a large number of URLs in one removal request, please also send an electronic copy of the notice to removals@google.com.

3. Provide information reasonably sufficient to permit Google to contact you (email address is preferred).

4. Provide information, if possible, sufficient to permit Google to notify the owner/administrator of the allegedly infringing webpage or other content (email address is preferred).

5. Include the following statement: "I have a good faith belief that use of the copyrighted materials described above as allegedly infringing is not authorized by the copyright owner, its agent, or the law."

6. Include the following statement: "I swear, under penalty of perjury, that the information in the notification is accurate and that I am the copyright owner or am authorized to act on behalf of the owner of an exclusive right that is allegedly infringed."

7. Sign the paper.

8. Send the written communication to the following address:

Google, Inc.
Attn: Google Legal Support, DMCA Complaints
1600 Amphitheatre Parkway
Mountain View, CA 94043

OR fax to:

(650) 963-3255, Attn: Google Legal Support, DMCA Complaints

Please note that a copy of each legal notice we receive is sent to a third-party partner for publication and annotation. As such, your letter (with your personal information removed) will be forwarded to Chilling Effects (http://www.chillingeffects.org) for publication. You can see an example of such a publication at http://www.chillingeffects.org/dmca512/notice.cgi?NoticeID=861. A link to your published letter will be displayed in Google's search results in place of the removed content.

Counter Notification

The administrator of an affected site or the provider of affected content may make a counter notification pursuant to sections 512(g)(2) and (3) of the Digital Millennium Copyright Act. When we receive a counter notification, we may reinstate the material in question.

To file a counter notification with us, you must provide a written communication (by fax or regular mail -- not by email, except by prior agreement) that sets forth the items specified below. Please note that you will be liable for damages (including costs and attorneys' fees) if you materially misrepresent that a product or activity is not infringing the copyrights of others. Accordingly, if you are not sure whether certain material infringes the copyrights of others, we suggest that you first contact an attorney. A sample counter notification may be found atwww.chillingeffects.org/dmca/counter512.pdf.

To expedite our ability to process your counter notification, please use the following format (including section numbers):

1. Identify the specific URLs or other unique identifying information of material that Google has removed or to which Google has disabled access.

2. Provide your name, address, telephone number, email address, and a statement that you consent to the jurisdiction of Federal District Court for the judicial district in which your address is located (or Santa Clara County, California if your address is outside of the United States), and that you will accept service of process from the person who provided notification under subsection (c)(1)(C) or an agent of such person.

3. Include the following statement: "I swear, under penalty of perjury, that I have a good faith belief that each search result, message, or other item of content identified above was removed or disabled as a result of a mistake or misidentification of the material to be removed or disabled, or that the material identified by the complainant has been removed or disabled at the URL identified and will no longer be shown."

4. Sign the paper.

5. Send the written communication to the following address:

Google, Inc.
Attn: Google Legal Support, DMCA Counter Notification
1600 Amphitheatre Parkway
Mountain View, CA 94043

OR fax to:

(650) 963-3255, Attn: Google Legal Support, DMCA Counter Notification

Account Termination

Many Google Services do not have account holders or subscribers. For Services that do, Google will, in appropriate circumstances, terminate repeat infringers. If you believe that an account holder or subscriber is a repeat infringer, please follow the instructions above to contact Google and provide information sufficient for us to verify that the account holder or subscriber is a repeat infringer.