E

WIPO

OSP/LIA/2
ORIGINAL: English
DATE: December 1, 1999

WORLD INTELLECTUAL PROPERTY ORGANIZATION
GENEVA

WORKSHOP ON SERVICE PROVIDER LIABILITY

Geneva, December 9 and 10, 1999

A LOOK BACK AT THE NOTICE-TAKEDOWN PROVISIONS
OF THE U.S. DIGITAL MILLENNIUM COPYRIGHT ACT
ONE YEAR AFTER ENACTMENT

prepared by Mr. Batur Oktay,
Corporate Counsel,
Adobe Systems Incorporated,
Seattle, Washington

and

Mr. Greg Wrenn,
Associate General Counsel,
Yahoo! Inc.,
Santa Clara, California

INTRODUCTION

In September of this year the United States deposited its instrument of accession to the WIPO Copyright Treaty ("WCT") and the WIPO Performances and Phonograms Treaty ("WPPT"). This act was the culmination of years of domestic and international debate on issues relating to the application of copyright law to the Internet. These debates—which proved to be some of the most intense lobbying in the copyright arena that the U.S. Congress has ever witnessed—eventually led to passage of the Digital Millennium Copyright Act ("DMCA"), which was signed into law on October 28, 1998.

The DMCA amends U.S. law in numerous ways. Most notably, the DMCA makes changes to the 1976 Copyright Act that permits the United States to ratify the WCT and the WPPT. Equally significant are the provisions in the DMCA that allow service providers to limit their potential monetary damages for the infringing activities of their users, subscribers, and account holders. The United States is the first country to address the application of copyright law in this area. It is therefore likely that the resolution of these issues set forth in the DMCA may provide a model for the rest of the world.

The first section of this article reviews the pertinent parts of the DMCA's service provider liability provisions. It summarizes the various threshold requirements and multiple, specific obligations that a service provider must satisfy in order to claim any one of four different liability limitations created by the DMCA. The second section of this article provides a synopsis of the experiences of content providers and service providers in implementing the DMCA's service provider liability provisions.

I. OVERVIEW OF THE DMCA

The Online Copyright Infringement Liability Limitation Act incorporated as Title II of the DMCA limits the remedies a content provider may seek from a service provider for copyright infringement under certain circumstances. The U.S. Congress determined that limiting the availability of remedies against a service provider is appropriate if a service provider satisfies three threshold prerequisites and additional specific conditions associated with functions/acts of: (1) transmitting, routing, and providing connections to infringing material (the "mere conduit" limitation); (2) system caching; (3) storing infringing material at the direction of a user (the "hosting" limitation); or (4) linking or referring users to infringing material (the "linking" limitation).

While the DMCA specifically states four circumstances where remedies against service providers are limited, the legislative history of the Act makes clear that it is intended neither to create new liabilities for service providers, nor affect any defense to infringement which otherwise might exist for a service provider under the Copyright Act or case law.

It is also significant to note that, while the DMCA limits remedies against service providers, it does not limit the rights of copyright owners or exclusive licensees to pursue a service provider's users, subscribers, or account holders for liability resulting from their direct acts of copyright infringement. Nor does the Act exempt service providers for acts of infringement that fall outside the four specified functions or prevent copyright owners or exclusive licensees from pursuing the service provider for damages caused by such acts.

A. Threshold requirements for "Service providers"

To benefit from any of the four limitations on remedies created by the DMCA, a service provider must qualify as a "service provider" and meet three threshold requirements.

To qualify as a "service provider" under the DMCA, the entity seeking to qualify must be one that offers the transmission, routing, or provision 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 sent or received;" or provides "online services or network access," or operate facilities therefor. The definition is specifically tailored to encompass the basic functions and services needed by users to access the Internet and enjoy its benefits. The definition does not distinguish between the kinds of businesses/persons that may provide such functions, thus it encompasses the owners and operators of corporate intranets, university networks and interactive websites, in addition to the more traditional service providers, OSPs and search engine firms that one might think of as "service providers." It does not encompass any and all persons using the Internet, merely those persons that perform the tasks that make the Internet available to users. Thus, a business using the Internet, for example to sell books, fresh fruit, or provide auction services, would not qualify as a service provider by the mere fact that their business uses the Internet to solicit business, conclude transactions, and deliver products or services by means of telecommunications networks.

Assuming the entity seeking to avail itself of the liability limitations in the Act passes the first hurdle and qualifies as a "service provider," it must then meet three additional threshold requirements: (1) it must have adopted and "*reasonably* implemented" a policy providing that it will terminate, "in appropriate circumstances," the accounts or subscriptions of "repeat infringers;" (2) it must inform its subscribers and account holders of its policy; and (3) it must accommodate and not interfere with "standard technical measures."[1]

Although the DMCA requires the service provider to terminate the accounts and subscriptions of repeat infringers, it is significant to note that, except in certain cases (discussed later), a service provider remains free to terminate service to someone who it believes in good faith is engaged in acts of infringement regardless of whether that individual has been found to previously infringe another's copyright. In addition, a service provider is free to contractually provide for termination of its users for any reason.

B. Four limitations on remedies

(1) Mere conduit limitation

A service provider that meets the threshold prerequisites for eligibility under the Act may, under certain circumstances, enjoy a limitation on remedies for copyright infringement

[1] "Standard technical measures" is defined in the Act as technical measures used by copyright owners to identify or protect their works. Under the Act, to qualify as a "standard technical measure," the technical measure must "have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process . . . ." In addition, the technical measure must be available to any person on reasonable and nondiscriminatory terms and must not impose substantial costs on Service providers or substantially burden their systems or networks.

for "transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for . . . [it,] or by reason of the intermediate or transient storage of that material in the course of such transmitting, routing, or providing connections . . . ." This limitation is directed at the fact that a "copy" capable of implicating a copyright owner's right of reproduction under the Copyright Act is created at multiple points over the Internet where a reproduction in transit is made temporarily.

To qualify for this limitation—which is commonly referred to as the "Mere Conduit" limitation—the service provider must be acting at "arm's length." To avail itself of the limitation on remedies and to prove that the service provider is performing such automatic arm's length functions, the service provider must present proof of five elements (1) the infringing transmission must have been initiated by or at the direction of a person other than the service provider; (2) the service provider's "transmission, routing, provision of connections, or storage" must have been carried out by "an automatic technical process without selection of the material by the service provider . . . ;" (3) the service provider must not select the recipients of the material except "as an automatic response" to another person's request; (4) the service provider must not maintain any stored copy of the material on its system or network in a manner that would allow nonrecipients to access the copy or for longer than necessary to allow the service provider to transmit, route, or provide connections for the material; and (5) the service provider must not modify the content while it was transmitted through its system or network.

(2) System caching limitation

The DMCA also limits the availability of remedies against a service provider for the intermediate and temporary storage of material on its system or network—commonly referred to as "system caching." For a service provider to avail itself of this limitation on remedies for system caching, the Act includes eight specific proof requirements that must be met by a service provider which otherwise has met the three threshold pre-requisites for eligibility under the Act. The first four conditions are generally applicable, while the following four apply only to specific situations:

(a) The allegedly infringing material at issue in a given suit must have been uploaded or made available online by a person other than the service provider.

(b) The material must have been transmitted to a third party at the request of the third party–such as when a user calls up a website.

(c) The material must have been temporarily stored on the service provider's network "through an automatic technical process for the purpose of making the material available to users of the system or network . . ." who requested the material from the person who originally made the content available. In other words, the content must have been "cached" as part of the technical process of transferring data from a location where it was originally stored (or transmitted from) to the computer of the person who is either the recipient of the email or listserv message (if the content traveled by email) or who directed their browser to a particular location on the web and thereby called up the information.

(d) The material must have been transmitted by the service provider to subsequent users without modification (*i.e.*, in exactly the same form as when it was originally posted or transmitted).

(e) In making the cached copy, the service provider must have complied with "rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data communications protocol for the system or network through which that person makes the material available . . . " This specific requirement is not applicable if the person who originally posted or transmitted the content uses these rules "to prevent or unreasonably impair the intermediate storage . . . " which is the subject of the specific limitation.

(f) The service provider must not "interfere with the ability of technology associated with the material" that returns information to the party which originally posted or transmitted it (such as cookies, which tell a website owner about visitors and allow site owners to customize the content they provide to specific users). This sixth requirement only applies, however, when the technology: (a) does not significantly interfere with the performance of the service provider's system or network or the intermediate storage of the material; (b) is consistent with generally accepted industry standard communications protocols; and (c) does not extract information from the service provider's system or network other than information that would otherwise have been available to the person who originally posted or transmitted the material, had subsequent users gained access to the material directly from that person.

(g) Where the party that originally posted, transmitted, or made available the infringing content conditioned access to the material on payment of a fee or provision of a password or other similar requirements, the service provider must permit access to the stored material "in significant part" only to users of its system or network that comply with those conditions.

(h) When infringing material is posted without the authorization of the copyright owner, the service provider must respond "expeditiously" to remove, or disable access to, the material . . . upon notification . . . . " The notification required, service provider's response to notification, and service provider's obligation to designate an agent are discussed below. This requirement only applies, however, if the material was previously removed from the website where it originated from or access to that website has been disabled or a court has ordered that the material be removed or access be disabled and the party giving notice includes a statement confirming these facts.

(3) Hosting limitation

Service providers that meet the threshold eligibility requirements may also enjoy a limitation on remedies for infringing material that is stored on their systems or networks at the direction of users if they can prove four additional requirements. This limitation on remedies is often referred to as the "hosting" limitation.

The first requirement of the hosting limitation on remedies mandates that a service provider either lacks knowledge of the infringement or took appropriate measures once it acquired such knowledge. This requirement essentially requires that the service provider lacks either actual or imputed knowledge of the infringement or has taken steps to remedy the situation once it learns of the infringement and may be satisfied if the service provider: (1) does not have actual knowledge that material or an activity using the material is infringing; or (2) "in the absence of actual knowledge, is not aware of facts or circumstances from which the

infringing activity is apparent . . . .;" or (3) upon learning of the infringement, acted "expeditiously to remove, or disable access to, the [offending] material . . . ."

The second requirement specifies that, when a service provider has the right and ability to control an infringing act, it must "not receive a benefit financially directly attributable to the infringing act." The third requirement provides that a service provider must remove or disable access to infringing material upon receipt of proper "notification" (as defined under the statute). The requirements for sending and responding to notifications are separately addressed below. The fourth requirement—which mandates that a service provider designate an agent to receive notification of claimed acts of infringement and that it make available certain contact information about the designated agent on its website "in a location accessible to the public . . . " and in a required filing with the U.S. Copyright Office—likewise is addressed below.

(4) Linking limitation

A service provider which otherwise meets the general threshold requirements under the Act may be avail itself of a limitation on remedies for linking or referring users to infringing material or activity by using "information location tools, including a directory, index, reference, pointer, or hypertext link . . . ." This limitation on remedies is often referred to as the "linking" or "information location tools" limitation.

To qualify for the linking limitation, a service provider must meet the four requirements of the hosting limitation discussed above. Specifically, (1) a service provider must not have actual knowledge or awareness of the infringement or, if it has either, it must promptly remove or disable access to the infringing material; (2) where a service provider has the right and ability to control the infringing activity, it must not "receive a benefit financially directly attributable to the infringing activity . . . ;" (3) the service provider must remove or disable access to infringing material upon receipt of proper notification; and (4) designate an agent upon whom proper notification may be served.

C. Notice and take down

In exchange for the four limitations on remedies set forth above, service providers agreed to provisions in the DMCA commonly referred to as "notice and take down." In general, the notice and take down procedures provide that when a copyright owner becomes aware of infringing material or infringing activity residing or taking place on a service provider's system or network that copyright owner may notify the service provider of the infringement and require the service provider remove or disable access to the infringing material or activity. This "notice and take down" procedure include several elements described below, notably designation of an agent, notification by the copyright owner, and counter notification by the alleged infringer.

(1) Designation of an agent

The caching, hosting, and linking limitations on remedies compel service providers to designate an agent to receive notifications. Service providers must designate an agent to receive notification of claimed acts of infringement and make available certain contact information about the designated agent on their websites "in a location accessible to the public …." and in a required filing with the U.S. Copyright Office. The contact information must include the name, address, phone number, and e-mail address of the designated agent, as

well as any other information that the Register of Copyrights may require (including a registration fee to cover the cost of publishing and maintaining a current directory of agents, which must be made available in both hard copy and electronic formats and made available over the Internet).

(2) Notification

A notification must be "a written communication" directed to the service provider's designated agent. Under the statute, a notification must include:

(a) A physical or electronic signature of a person authorized to act on behalf of the copyright owner or exclusive licensee.

(b) Identification of the copyrighted work claimed to be *infringed*. If a notice refers to multiple works posted at a single location, it is sufficient to include a representative list of works infringed at the site.

(c) Identification of the material claimed to be *infringing* together with "information reasonably sufficient to permit the service provider to locate the material." For purposes of the information location tools limitation, the notification must also identify the reference or link to the material or activity claimed to be infringing and information "reasonably sufficient" to permit the service provider to locate the reference or link.

(d) Information "reasonably sufficient" to permit the service provider to contact the complaining party. Such information may include the complaining party's address, telephone, or email address.

(e) A statement that the complaining party believes, in good faith, that the copyrighted material identified is being used in a manner that is not authorized by "the copyright owner, its agent, or the law." and

(f) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

All six requirements do not necessarily have to be met for a particular notification to be considered proper. The Act merely requires "substantial" compliance with these requirements.

In response to a notification, a service provider's obligations will vary depending on the type of infringement alleged. A service provider must expeditiously remove or disable access to allegedly infringing material that has been cached, but only if the material first was removed from the originating site (or access to it was blocked). A service provider likewise must respond *expeditiously* to remove or disable links or similar information location tools or material stored on its system or network by a user to qualify for either the linking or hosting limitations.

(3) Counter notification

Upon receipt of a notification, a service provider will be exempt from liability to its subscribers for its good faith removal of or disabling access to allegedly infringing content

residing on its server at the direction of the subscriber. This exemption only applies with respect to material residing at the direction of a subscriber, however, if the service provider "take[s] reasonable steps *promptly* to notify the subscriber that it has removed or disabled access to the material" and thereby allows the subscriber to respond to the infringement alleged in the notification. A subscriber's response is referred to in the statute as a "counter notification."

Like a notification, a counter notification, to be considered proper, must be "a written communication provided to the service provider's designated agent . . . " and satisfy certain content requirements. Specifically, a counter notification must include:

(a) A physical or electronic signature of the alleged infringer;

(b) Identification of the material that was removed or disabled by the service provider and the location where the material appeared before it was removed or access to it was disabled;

(c) A statement under penalty of perjury that the alleged infringer has a good faith belief that the material at issue was mistakenly removed or misidentified; and

(d) The alleged infringer's name, address, and telephone number and a statement that the alleged infringer consents to the jurisdiction of the federal district court for the judicial district in which the address it provides is located and that it will accept service of process from the person who provided the original notification. If the alleged infringer is located outside the United States, the alleged infringer must include a statement that it consents to the jurisdiction of any U.S. federal district court in which the service provider may be found.

The counter notification—like the notification—need only "substantially" include the information required by the statute.

Upon receipt of a counter notification, a service provider must promptly provide the original complainant with a copy of the counter notification and inform him that it will replace the removed material or cease disabling access to it within ten business days. The original complainant must then file suit within the ten-day period to obtain a court order restraining the subscriber from engaging in infringing activity if it wants to prevent access to the material from being restored. Absent evidence that a lawsuit has been filed "seeking a court order to restrain the subscriber from engaging in infringing activity . . ." a service provider is required by the Act to "replac[e] the removed material and cease disabling access to it not less than ten, nor more than fourteen, business days following receipt of the counter notice . . . ."

(4) <u>Service provider protections against misrepresentations contained in a notification or counter notification</u>

The notice and take down procedures set forth in the Act relieve service providers of any obligation to evaluate the merits of a dispute . To minimize the likelihood that fraudulent notifications or counter notifications would be filed, the Act provides that both complainants and alleged infringers may be subject to liability if they make material misrepresentations in a notification or counter notification. Specifically, any person who "knowingly materially misrepresents" that material or activity is infringing or was removed or disabled by mistake or

misidentification may be held liable for damages, including costs and attorneys' fees, in an action brought by an alleged infringer, a copyright owner or authorized licensee or a service provider injured by a service provider's reliance on the misrepresentation.

D. Additional provisions

In addition to the four liability limitations and the notice and take down procedures discussed above, the DMCA also includes several other provisions aimed at improving the interaction between copyright law and the Internet and the parties and technologies that intertwine the two.

(1) Service provider protections against removing or disabling access to material it believes to be infringing

A service provider that otherwise has met the threshold requirements set forth may be entitled to a broad exemption for its good faith disabling of access to or remove of material believed to be infringing (even when a notification has not been submitted). Specifically, the Act immunizes service providers from liability "to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts and circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing."

Under the protections afforded by this section of the DMCA service providers may act on their own initiative or in response to customer or other third -party complaints to remove or disable access to content believed to be infringing without fear of being held liable for a legal claim made by the person whose material has been removed or access to disabled. This exemption applies to any claim that could conceivably be made against a service provider for removing or blocking access to content, such as tort or breach of contract claims.

The one exception to this "good faith" exemption arises when a service provider disables access to or removes the allegedly infringing material pursuant to a notification. Once a notification has been received, however, a service provider must comply with the specific requirements governing counter notification—as discussed above—for this exemption to apply.

It is significant to note that this "good faith" exemption applies regardless of whether the removed or disabled material is ultimately found to be infringing. Further, while the DMCA—and the "good faith" exception in particular—creates incentives for service providers to monitor and block content, they are not required to do so or to seek facts indicating infringing activity, except to the extent consistent with a "standard technical measure" (as defined above). Nor is a service provider required to disable access to or remove any material where doing so is prohibited by law.

(2) Subpoenas to identify infringers

The DMCA also includes provisions that enable the copyright owner to determine the identity of an online infringer. Specifically, the DMCA permits a copyright owner or person authorized to act on the owner's behalf to request a clerk of "any United States district court" to issue a subpoena to a service provider requiring identification of an alleged infringer. Each request must include a copy of the notification, a proposed subpoena, and a sworn declaration

stating that the copyright owner will only use the information obtained from the subpoena for protecting its rights under the Copyright Act.

If the request contains each of these elements and the notification is proper, a subpoena will issue. The subpoena will authorize and order the service provider to expeditiously disclose to the copyright owner (or person authorized by the copyright owner) information sufficient to identify the alleged infringer, to the extent that such information is available to the service provider. Upon receiving the subpoena, the service provider must "expeditiously" disclose the information required by the subpoena, notwithstanding any other provision of law and regardless of whether the service provider responds to the notification. To "the greatest extent practicable . . . ," the procedures for issuing, delivering and enforcing Service provider subpoenas are to be governed by those provisions of the Federal Rules of Civil Procedure governing the issuance, service and enforcement of a subpoena *duces tecum*.

(3) Specific provisions relating to the liability of nonprofit education institutions

In addition to the four limitations created for all service providers, Nonprofit Education Institutions (NEIs) may benefit from special rules that may immunize universities for the infringing acts of faculty members or graduate students which otherwise might be imputed to an NEI, as employer, and prevent it from benefiting from the mere conduit, system caching, or hosting limitations.

Under this special NEI limitation, the acts or knowledge of a faculty member or graduate student will not be imputed to the "public or other nonprofit institution of higher education" that employs her if: (1) the "faculty member or graduate student" is "an employee of such institution . . . performing a teaching or research function . . . .;" (2) the faculty member's or graduate student's infringement does not involve the provision of online access to instructional materials that are or were required or recommended by that faculty member or graduate student within the proceeding three-year period for a course taught at the NEI; (3) the NEI has not received more than two notifications, which claim copyright infringement by such faculty member or graduate student, within the three-year period; and (4) the NEI provides all users of its system or network with informational materials that accurately describe and promote compliance with U.S. copyright laws.

E. Limited injunctive relief available against service providers

The DMCA authorizes limited injunctive relief against service providers who comply with the Act's requirements to deny access to infringers and block infringing content, both in the United States and overseas. Specifically, a court may grant only three specific forms of equitable relief against a service provider (other than a service provider that is also an NEI) which has met the burdens of proof and qualifies for the limitations on remedies under the system caching, hosting, or linking limitations:

(1) a court order restraining the service provider "from providing access to infringing material or activity residing at a particular site on the provider's system or network;"

(2) a court order requiring a particular infringer's account or subscription be terminated by the service provider in order to deny it access to the system or network; or

(3) such other injunctive relief as the court may consider necessary to prevent or restrain infringement of specific material 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."

By contrast, a court may only enjoin a service provider (that is not also an NEI) whose liability is otherwise limited under the mere conduit limitation from providing access to a subscriber or account holder who is using the service provider's services to engage in infringing activity by terminating its account or restraining it from providing access (through reasonable steps to be specified in the court order) to infringing material at a particular online location outside the United States. This provision is significant for copyright owners, in that it specifically authorizes a court to compel a service provider subject to jurisdiction in the United States to block access to content which would be infringing under U.S. law, even though the content is located overseas in a country where it may not be deemed infringing under that country's laws or is located on a server owned by an entity which may be beyond the jurisdiction of a U.S. court.

In determining whether to grant injunctive relief against a service provider that has met the burdens of proof established by the statute for that service provider to qualify for the limitation on remedies , the DMCA directs the court to weigh substantially the same factors a court would weigh in granting any injunctions, including: (1) whether the order would significantly burden either the service provider or the operation of its system or network; (2) the magnitude of harm likely to be suffered by the copyright owner if steps are not taken to prevent or restrain the online infringement; (3) whether implementation of a proposed injunction would be technically feasible and effective and would not interfere with access to noninfringing material at other online locations; and (4) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.[2]

The DMCA further provides that injunctive relief may only be granted where a service provider is given notice and the opportunity to appear, except for orders "ensuring the preservation of evidence or other orders having no material adverse effect on the operation of the service provider's communications network."

II. IMPLEMENTATION OF THE DMCA: EXPERIENCES OF CONTENT PROVIDERS AND SERVICE PROVIDERS

A. Notice and take down under the DMCA: The content provider perspective

(1) Content provider views on notice and take down procedures

Overall, the notice and take down procedures in the DMCA are relatively straightforward. The first step in the notice and take down process—at least from the content provider’s viewpoint —is to locate the service provider and that service provider’s contact information. Because the content providers cannot readily recognize the owner of a site from

[2] The considerations for granting injunctive relief and requirement for notice apply equally to Service providers that are also NEIs, although the limitations on the specific forms of injunctive relief which may be granted do not apply to NEIs.

the URL alone, many content providers use the WHOIS database[3] to determine the identity of the service provider. After determining the identity of the service provider the content provider should review the Copyright Office list of registered agents to locate that service provider's specified contact information.

At times it is difficult to locate a service provider's contact information. Some service providers want to remain hidden, and do a good job of it. It is therefore imperative that domain name registries maintain good records of the identities of their registrants and make this information readily available and easily accessible to content providers so that content providers are not hindered from locating and contacting the appropriate service provider to take infringing material down.

Once the contact information is ascertained, the content provider prepares a notification, which includes certain information required by the DMCA ("content requirements"), and sends it to the service provider's designated agent. The content requirements under the DMCA are clear and simple enough that most content providers have not been required or asked to provide more detailed information to a service provider before the infringing material is removed. Adobe has never had to provide such additional information.

Most of the sites about which content providers have contacted service providers through the DMCA notice and take down procedure are free sites. In other words, these free sites permit users to post material without charge. The service providers hosting these free sites do not monitor what is being posted. Given the free access and the lack of monitoring by the service provider of these sites, they have become a "breeding ground" for infringing material; there are literally hundreds of free sites on which infringing material can be found.

Content providers have used several different methods of providing notification, including e-mails, letters, and telephone calls to the service provider's designated agent. While a variety of methods have been used, the most common method of providing notice is e-mail simply because it is the easiest and quickest method of contacting a service provider. On occasion, content providers have found that a service providers may require that a notification be faxed or mail to them, so they have a hard copy of the notice for their records. However, this seems to be the exception rather than the rule.

The notifications are normally sent to a mailbox identified by many service providers as an "abuse" mailbox. How quickly a notice is seen and acted upon by a service provider thus often depends on how frequently a service provider checks its abuse inbox. It has been the content providers' experience to date that there has not been a significant time lag between the sending of a notification to a service provider and the service provider becoming aware of the notification. Normally, service providers have responded to the notices within a period of twenty-four hours, although Adobe has experienced both shorter and longer time lags. Thus it is Adobe's perception that most service providers review their abuse mailboxes at least daily. In some instances service providers have responded within a few hours, and in the worst case

---

[3] http://www.networksolutions.com/cgi-bin/whois/whois/. The data base of registered agents made available by the U.S. Copyright Office at http://www.loc.gov/copyright/onlinesp/list/index.html lists service providers by business name and not by domain name, so use of the WHOIS database is usually needed to try and identify the service provider's business name when all that is known by the content provider is the domain and URL of the offending material.

scenario (other than complete failure to respond), a service provider did not respond to an Adobe notice for a period of two weeks.

Upon receipt of notice from a content provider, most service providers will provide return notice back to the copyright owner once they have taken down infringing material. Although this is not required by the DMCA, it is extremely useful to content providers because it allows them to determine whether the infringing material identified in a notification has been removed (or access to it disabled) without having to revisit every site containing infringing material for which a notification has been sent.

(2) Problems with notice and take down

Content providers have identified several problems with the DMCA's notice and take down procedures. Among the most significant problems is the time lag between notice and take down; it often takes too long for a service provider to take the infringing material down. Although the DMCA requires "expeditious" removal by a service provider upon receiving notice, it fails to specify the length of time permitted for such removal. As a result, service providers often will not take down infringing material for days or in some cases weeks.

Long lag time between receipt of a notification and removal or disabling of access to the infringing material by a service provider can be devastating to a content provider. In the case of freely downloadable software in particular, failure to promptly take down infringing software can result in the distribution of thousands of copies of illegal software. For instance, with fast lines, an individual can download an Adobe software application like Photoshop in a matter of minutes. Thus, if an infringing copy of Photoshop is on a website for 24 hours before being taken down, literally hundreds if not thousands of downloads may be performed. In one case where Adobe obtained the download logs from a site that had been up for six months, there were over 100,000 downloads of Photoshop during that time, with a street value of US$60 million. The timing of the take down is therefore of significant concern to content providers and an area of implementation of the DMCA that needs to be improved.

Another problem affecting content providers is the manner of the service provider's take down. Often a service provider's method of "removing" infringing material will be to freeze the page or pages, in such a way that the pages can be viewed but not accessed. Despite the fact that infringing material cannot be downloaded from these frozen sites, page freezing is of minimal effectiveness because users can still access and view the frozen pages to locate the infringer's contact information, and contact the infringer directly to obtain the infringing material. Hence, an illegal transaction can take place later, perhaps on another site.

A third problem is the significant burden placed on content providers by the notice and take down process. Adobe has had to employ a team of internal investigators who do nothing but surf the Internet for infringing material, some of which is very difficult to find. Other content providers have had to hire staff to do the same. Adobe's investigators send 40-90 take down notices per day. And as Adobe expands its program, that number will only grow. The employment of investigators to constantly monitor the internet is time consuming and costly, and it only scrapes the very surface layers of the problem, which is as big as the internet itself.

Despite these problems, content providers recognize that the notice and take down procedures under the DMCA provide them with an additional tool to combat software piracy and copyright infringement. The process has worked well especially in light of the fact that service providers have cooperated in almost every single case. Of course, the benefits

obtained from the notice and take down procedures in the DMCA must be balanced against the magnitude of the infringement problem. For instance, in 1997, there were approximately 100,000 warez[4] pages on the internet. In 1998 that number ballooned to 900,000. And now, in 1999, there are approximately two million warez pages on the world wide web. Is notice and take down sufficient to deal with this problem? Obviously not, because a content provider cannot possibly locate and review two million web pages and contact every service provider involved. In addition, when infringing material is removed from a site, it usually pops back up on another site within a matter of hours, and in some instances, minutes. With the prevalence of IRC and client/server software like Hotlines that allows end users to make infringing material available directly from their own computers (as opposed to via a service provider's server), this material can be moved virtually instantly. Thus, while the notice and take down procedures have proven to be a useful tool to fight copyright infringement, from the content providers viewpoint much more needs to be done to combat this overwhelming problem.

B. Notice and take down under the DMCA: The service provider perspective

The Internet is growing at an astounding pace. Recent reports show that in the first half of 1999, Internet portals[5] added millions of monthly visitors with double-digit growth in this sector. [6] In September 1999, for example, Yahoo! recorded over 105 million unique individual visitors to its worldwide network, compared with just over 80 million unique visitors in June 1999.[7]

Yahoo! has had extensive experience handling take down requests in the United States under the DMCA procedures. Yahoo!'s designated copyright agent under the DMCA handles several thousand notices each calendar quarter. The sections below describe the pros and cons, from the service provider's perspective, of notice and take down under the DMCA.

(1) The advantages of a notice and take down system

There are several advantages to the DMCA's structured notice and take down system from a service provider perspective. First of all, it provides copyright owners[8] a clear procedure, and service providers a clear "safe harbor," that enables both parties to quickly and efficiently address allegations that users of the service provider's system are infringing copyrights. Legal claims involving other areas of law where no established procedure exists can cause more confusion and work among the parties, and without the clear incentive of a safe harbor provision, service providers are less likely to "take sides" between the content provider and the user (this results in no take down). Trademark infringement claims, for

---

4 "Warez" is a term widely used in pirate subcultures to denote illegal copies of commercially available computer software, often including "cracked" versions of software, that is versions from which copy-protection has been stripped.

5 A portal is a gateway to the Internet, a web site that users normally go to first when visiting the Internet because the site has services such as an index of third-party web sites by topic or a search engine for finding links to other web sites by keyword. Portals often have other tools that users use frequently, such as email and a personalized selection of news and financial information.

6 Source: Media Metrix, July 1999.

7 Yahoo! Inc. Press Release, October 6, 1999.

8 The reference to "copyright owners" in this section is used as a short reference to copyright owners and their representatives, and exclusive licensees and their representatives, who have standing to assert copyright infringement claims under the DMCA procedures.

example, are less likely to result in take down compared with copyright infringement claims at Yahoo! because there is no specified procedure at law and no statutory safe harbor to encourage processing in a particular manner.

Another positive aspect of the DMCA procedure is that it creates additional liability on the part of the copyright owner for any knowing misrepresentations made in relation to a take down request. This is important because it helps to discourage baseless complaints that often are made not to protect intellectual property rights, but rather to harass or silence a critic.

The DMCA's streamlined procedure for obtaining a subpoena also has a positive effect for all potential participants in the process, including the courts. Copyright owners are able to obtain information under a DMCA subpoena much faster and less expensively than alternative methods, and with less burden on the court system.[9] Service providers often may not be able to provide identifying information related to individual users without a subpoena, due to privacy policies and other considerations; issuance of a valid subpoena relieves the service provider of liability it might otherwise face for disclosing such information. Further, for users, the requirement of a subpoena means that certain requirements must be met that prevent third parties from having casual or unwarranted access to the user's personal information.[10]

The DMCA also allows service providers to comply with take down requests from copyright owners without being caught in a crossfire between claims by copyright owners and claims by users. Without these safe harbor protections, service providers would be less likely to comply with take down requests, since that could give rise to possible liability to users. The DMCA explicitly relieves service providers from any liability that might exist to users when the service provider complies with a proper take down request. It also gives service providers immunity from liability for monetary damages on claims by the copyright owner. Just as importantly, it preserves all rights and defenses a service provider may have if the service provider chooses not to comply with a take down request. This gives service providers the option to decline the safe harbor and rely on all available defenses—an option service providers may need in order to protect users from the occasional baseless or improper take down demands. This can be important when, as a practical matter, most individual users do not have the resources to defend against well-financed copyright owners, even if the users have a valid defense. Last, but not least, the DMCA clarifies the circumstances in which service providers who merely route, cache, host or link to allegedly infringing material are not liable—including a specific provision directed at "information location tools" such as Yahoo!'s search engine—so that performing the basic functions required to effectively operate within the Internet infrastructure do not subject service providers to liability for the conduct of individual users on the network.

---

[9] Before the DMCA, copyright owners often faced the prospect of filing a civil lawsuit in the United States in federal courts permitting "John Doe" complaints, i.e., lawsuits directed at unnamed defendants, and then petitioning the court for permission to issue a subpoena to service providers to discover the identity of the individuals responsible for the material at issue. This process could take several weeks to complete and cost thousands of dollars.

[10] In addition to the usual rules governing the issuance of a subpoena in civil cases in U.S. courts, additional regulations can apply to restrict access to personal information related to Internet users, such as the restrictions on governmental entities' access to such information under the Electronic Communications Privacy Act, 18 U.S.C. § 2701 (1988).

Finally, the DMCA notice and take down provisions are useful in what they do *not* do, and that includes refusing to impose any obligation on service providers to monitor user activity prior to notice from the rights holder. When service providers can have tens of millions of active users, all capable of creating and posting web pages, offering items for sale via auctions, emailing large files to others, and posting advertisements on message boards, it is simply impossible to screen material for possible copyright infringement (or defamatory material, or trademark infringement, etc.) ahead of time, even assuming service providers could distinguish, say, legal software offered by authorized resellers from counterfeit or parallel import products. The DMCA also is useful in that it avoids setting a fixed amount of time for a service provider to respond to a take down request, requiring instead that take down occur "expeditiously." At Yahoo!, most take downs occur within 24 to 48 hours of receiving notice, but at times it can take longer. For example, if a content provider suddenly starts sending a large volume of take down requests, it may create a backlog as Yahoo! employees review the requests and the posted material at issue. Delays can also occur if the content provider fails to provide all the required information in the notice—especially if the posted material is not specifically identified using something like a URL (the Internet's Universal Resource Locator pointing to a particular web page) or a message ID number on a message board. Based on records kept by Yahoo!, five to six percent of all requests received fail to comply or substantially comply with the DMCA notice requirements in terms of contents, resulting in no action by Yahoo! or delays until a proper notice is received.

(2) Problems with notice and take down

Despite the significant advantages of a notice and take down system, there are still some problems and unanswered questions that have been encountered.

"Electronic Signatures." One lingering issue with the notice and take down provisions of the DMCA is in the area of authentication of a take down request. The DMCA refers to the requirement of a physical or "electronic signature" of a person authorized to act on behalf of the copyright owner or exclusive licensee.[11] Presumably the U.S. Congress intended to refer to something more commonly known as "digital signatures" available on the Internet, where the use of private and public encryption keys help to verify the authenticity of a message.[12] But the reference to "electronic" signature has resulted in some problems for Yahoo! because most of the DMCA notices come via email, and most of those emails have no "digital signature" that could be used to verify the identity of the sender. When Yahoo! has raised this issue in the past questioning the sufficiency of notices, the complaining parties normally argue that the "signature" of a normal email message—that is to say the few lines of text a user can have inserted at the end of messages automatically, or even a manually typed name at the end of an email message—constitutes an "electronic signature" for the purposes of a DMCA notice.

---

[11] 17 U.S.C. § 512(c)(3)(A)(i).

[12] Digital signature technology involves the use of public and private key encryption. The private key, a series of numbers, is kept secret by the owner and used to encrypt a message. The public key, another series of numbers generated along with the private key, is made available by the owner and can be used by anyone to decrypt the message. Since the public key will only decipher messages encrypted using the private key, it can be used to verify that the message came from the owner of the private key. Hence, the message has a "digital signature" by virtue of being encrypted with the private key.

The problem with simple email signatures is that email accounts can be set up quickly and easily on the Internet through email services offered by numerous providers, with virtually no technical limitation on the name selected for the email account other than whether the exact same name has been taken before. The email addresses operate as pseudonyms, often with no readily available way to confirm the actual identity of the owner of the account. Further, email addresses can be "spoofed," that is to say, messages appear to be from another account for which the user has no access, such as "directorgeneral@wipo.int." Consequently there can be times when Yahoo! may have questions about the authenticity of a message and whether a proper take down notice has been received from the copyright owner. The DMCA procedure could be substantially improved by requiring greater indicia of authenticity in messages than just an "electronic signature."

Sham Infringement Claims. Another problem that arises under the DMCA notice and take down procedure is the occasional abuse by some content providers. The vast majority of take down requests are made in good faith. Over fifty percent of the requests involve what appear to be outright piracy of content providers' copyrighted material—illegal "warez" sites offering pirated software, for example. An additional group of requests involve what appear to be good faith allegations of copyright infringement not involving piracy, such as a photographer alleging that his or her photograph has been used on a web site without his or her authorization. Remaining claims—estimated at approximately five percent—appear to be "sham" claims used to silence or harass critics by relying on questionable copyright claims. Companies have demanded that Yahoo! take down sites that criticize a company's product, for example, by objecting to quotes on the site taken from the company's product packaging. The Church of Scientology also continues a very aggressive campaign against online critics and dissidents who question the Church's positions and teachings, often relying on copyright claims to shut down a web site.

As a practical matter, notice and take down begins and ends the debate over whether a site stays up. Most service providers have little incentive to incur the costs and risks of litigation and will opt for the safe harbor, taking the site down. Users can provide a "counter notification"[13] giving the copyright owner 10 days to obtain a court order to keep the site down, but very few users choose this option in Yahoo!'s experience. Those that do are normally in a position to negotiate some form of compromise with the copyright owner. For example, the take down request may relate to a competitor's use of the complaining party's packaging text or product images for comparison purposes, and the competitor may feel it has the resources and legal arguments to justify use of the material. These sorts of cases involving counter notification by Yahoo! users have *all* been resolved without the need for further court action. The vast majority of cases, however, totaling thousands every quarter at Yahoo! involve no counter notification; the materials are taken down and stay down. This may be expedient and efficient, but to some extent it represents a "might makes right" resolution that gives little or no consideration to the validity of the copyright interest being asserted, its ownership, the permissible scope of protection, or defenses such as parody, fair use, de minimis use, and so on.

The DMCA procedure also creates some additional work and burden for many service providers. Responding to take down requests can be a significant expense and effort. Many service providers are relatively small companies in very competitive markets where the added expense is more than just an inconvenience and can have a serious effect on the business.

---

[13] 17 U.S.C. § 512(g)(3).

Other service providers, depending on the nature of the services offered, may notice little or no effect on their business. In Yahoo!'s case, Yahoo! has one full-time designated Copyright Agent who can no longer keep up with the volume of take down requests received. He has found it necessary to train three additional backup resources to help him cover the workload. He also is supported by over 15 full-time Customer Care employees, two full-time attorneys, and one paralegal, all of whom handle a range of complaints including alleged copyright infringement as well as allegations of defamation, trademark infringement, and other claims.

It is probably true that many of these people would still be needed even without a DMCA procedure, since content providers asserted take down requests before enactment of the DMCA, at times even resorting to litigation against service providers to secure their cooperation.[14] But the DMCA still imposes a substantial burden that requires service providers to hire additional personnel and equip them with computers and technology necessary to access the system and remove material that is subject to take down requests. Further, the DMCA also keeps service providers in the middle of communications between the content provider and the user longer than is necessary. The service provider is responsible for notifying the user upon receipt of a take down request if action is taken, and must wait to see if a counter-notification is returned, in which case the service provider must forward that notice to the content provider and then wait to see if the content provider obtains an injunction. This may sound easy in isolation, but if you are tracking a few thousand cases every quarter it can be challenging. The trend is for these complaints to increase based on Yahoo!'s experience,[15] not just because of the millions of new users signing up for Internet services each month, but because the content providers are becoming more familiar with the process and more efficient at using it. It is much easier for a content provider to send large volumes of take down requests using a form than it is for a service provider to properly process the requests. A single content provider in the software field has generated as many as 90 take down requests in one day directed at a single service provider, and has sustained notices at a rate of over 40 per day to a single service provider for a period of months. Service providers like Yahoo! are having more trouble keeping up with the increasing volume of requests and would find it easier if more of the burden of communicating was on the content providers and the users, and service providers were not responsible for forwarding so much of the communication between the parties. For example, once a service provider receives a take down request and notifies the user,[16] the service provider should have no further obligation to forward messages or respond to the parties except to watch for a copy of a counter notification and service of a copy of an injunction if one is obtained.

---

[14] In late 1996, the Software Publishers Association on behalf of three of its members filed suit against certain ISPs, including Community Connexion (a.k.a. C2Net), who either ignored or declined to remove allegedly infringing material posted by users of the ISP. The controversial cases illustrated the need for greater clarity and balance of considerations between the interests of content providers, service providers, and users who post and maintain content on the Internet.

[15] During the months of July 1999 through September 1999, notices to Yahoo!'s designated copyright agent increased 61% while growth in the number of the monthly visitors was substantially lower by comparison at approximately 31%.

[16] Most service providers do not object to providing initial notice to the user since the public may not know how to communicate with the user—email addresses or other contact information often is missing from posted materials. The service provider usually will have non-public contact information for the user by which at least an email notice can be sent, assuming the user has provided accurate contact information to the service provider in the past.

Finally, the DMCA procedure is not as clear as it might be on certain disclosure issues. For example, while the statute requires that any counter notification from the user be forwarded to the copyright owner, it does not state that the copyright owner's initial take down request must be forwarded to the user. A surprising number of take down notices received by Yahoo! include requests that the copyright owner remain anonymous to the user. Yahoo! declines requests for anonymity on the basis that it may prevent the user from effectively responding by counter notification, and it also seems fundamentally unfair; nevertheless it would be useful for legislation to explicitly state that take down notices may not be made on any condition of anonymity.

These are the problems evident at the moment. It is important to remember that the DMCA is still relatively new legislation and take down requests are still growing at a rate faster than the growth in the user base.[17] The coming months and years may well bring to light new areas of concern for all parties to the process.

---

[17] See footnote 16, supra.[17] "Standard technical measures" is defined in the Act as technical measures used by copyright owners to identify or protect their works. Under the Act, to qualify as a "standard technical measure," the technical measure must "have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process . . . ." In addition, the technical measure must be available to any person on reasonable and nondiscriminatory terms and must not impose substantial costs on Service providers or substantially burden their systems or networks.

[17] The considerations for granting injunctive relief and requirement for notice apply equally to Service providers that are also NEIs, although the limitations on the specific forms of injunctive relief which may be granted do not apply to NEIs.

[17] http://www.networksolutions.com/cgi-bin/whois/whois/. The data base of registered agents made available by the U.S. Copyright Office at http://www.loc.gov/copyright/onlinesp/list/index.html lists service providers by business name and not by domain name, so use of the WHOIS database is usually needed to try and identify the service provider's business name when all that is known by the content provider is the domain and URL of the offending material.

[17] "Warez" is a term widely used in pirate subcultures to denote illegal copies of commercially available computer software, often including "cracked" versions of software, that is versions from which copy-protection has been stripped.

[17] A portal is a gateway to the Internet, a web site that users normally go to first when visiting the Internet because the site has services such as an index of third-party web sites by topic or a search engine for finding links to other web sites by keyword. Portals often have other tools that users use frequently, such as email and a personalized selection of news and financial information.

[17] Source: Media Metrix, July 1999.

[17] Yahoo! Inc. Press Release, October 6, 1999.

[17] The reference to "copyright owners" in this section is used as a short reference to copyright owners and their representatives, and exclusive licensees and their representatives, who have standing to assert copyright infringement claims under the DMCA procedures.

[17] Before the DMCA, copyright owners often faced the prospect of filing a civil lawsuit in the United States in federal courts permitting "John Doe" complaints, i.e., lawsuits directed at unnamed defendants, and then petitioning the court for permission to issue a subpoena to service providers to discover the identity of the individuals responsible for the material at issue. This process could take several weeks to complete and cost thousands of dollars.

[17] In addition to the usual rules governing the issuance of a subpoena in civil cases in U.S. courts, additional regulations can apply to restrict access to personal information related to Internet users, such as the restrictions on governmental entities' access to such information under the Electronic Communications Privacy Act, 18 U.S.C. § 2701 (1988).

[17] 17 U.S.C. § 512(c)(3)(A)(i).

[Footnote continued on next page]

III. CONCLUSION

While the DMCA passed a little over a year ago, content and service providers alike have taken steps in implementing and utilizing the notice and take down provisions in the Act. From both industries' standpoint there have been bumps along the way as many businesses continue to struggle with the appropriate balance between resources and implementation. But the interested parties have also found numerous benefits from the notice and take down procedures in the DMCA that have helped to foster greater cooperation between the industries affected, and less burden on the court systems handling copyright infringement claims.

[End of document]

[Footnote continued from previous page]

[17] Digital signature technology involves the use of public and private key encryption. The private key, a series of numbers, is kept secret by the owner and used to encrypt a message. The public key, another series of numbers generated along with the private key, is made available by the owner and can be used by anyone to decrypt the message. Since the public key will only decipher messages encrypted using the private key, it can be used to verify that the message came from the owner of the private key. Hence, the message has a "digital signature" by virtue of being encrypted with the private key.

[17] 17 U.S.C. § 512(g)(3).

[17] In late 1996, the Software Publishers Association on behalf of three of its members filed suit against certain ISPs, including Community Connexion (a.k.a. C2Net), who either ignored or declined to remove allegedly infringing material posted by users of the ISP. The controversial cases illustrated the need for greater clarity and balance of considerations between the interests of content providers, service providers, and users who post and maintain content on the Internet.

[17] During the months of July 1999 through September 1999, notices to Yahoo!'s designated copyright agent increased 61% while growth in the number of the monthly visitors was substantially lower by comparison at approximately 31%.

[17] Most service providers do not object to providing initial notice to the user since the public may not know how to communicate with the user—email addresses or other contact information often is missing from posted materials. The service provider usually will have non-public contact information for the user by which at least an email notice can be sent, assuming the user has provided accurate contact information to the service provider in the past.

[17] See footnote 16, supra.