# The COMPUTER & INTERNET Lawyer

Volume 20 ▲ Number 5 ▲ MAY 2003

Arnold & Porter, Editor-in-Chief


## Features



## Current Developments




ASPEN PUBLISHERS

# Don't Shoot; I'm Just the Web Site Host!

**by Joel Voelzke**

Imagine this stomach-churning scenario. Your company operates a Web site hosting business, and one day you receive a call from a lawyer who says that her client is very upset about one of the Web sites that your company hosts. She claims that the offending Web site is using her client's trademark, or copyrighted images, or that the site libels her client, or that there is something else legally objectionable about the site. She demands that you immediately disconnect the Web site and says that she will sue you if you do not. If she is a government lawyer, she may even threaten to criminally prosecute you if you do not disconnect a site that she says is being used to sell narcotics or transmit child pornography. Assuming her to be a reasonable individual, you explain to her that your company merely hosts Web sites that were created by others and that you had no role in creating or maintaining the site. She then threatens to sue or bring criminal charges against you anyway.

You are not sure whether a party really can haul your company into court or whether your company can be criminally convicted for merely hosting a troublesome Web site. You realize, however, that because the offending material physically resides on your servers, and it is your servers that actually send the material out over the Internet, maybe she has a point. Maybe somehow in the eyes of the law you could be held at least partly responsible for that content. You also know that you would rather not find out the hard way. You call your hosted client and ask if he would be willing to take his site down voluntarily or at least modify it to remove the questionable material. Your client refuses. In fact, he insists that he is doing nothing wrong and threatens to sue your company for breach of your hosting contract and interfering with his business if you disconnect the site.

Now you are stuck between the proverbial rock and a hard place. No matter what you do, one or the other party is going to sue you or, worse, try to send you or your client to jail. What is an innocent Web site host to do? What actions should you be taking now, including updating your terms of service and your hosting contract, to keep from getting caught in future legal crossfire between warring parties over the content of a Web site?

Whether a Web site host can be held liable for the content of a hosted site, and what it should be doing now to avoid legal trouble, will depend heavily on the cause of action asserted by the plaintiff. For certain causes of action, some courts have said that Web site hosts can indeed be held liable for not disconnecting offending sites. For other causes of action, the answer lies at the opposite end of the spectrum. Congress has given Web site hosts and other Internet Service Providers (ISPs) absolute immunity from suit. The host might be able to recover all of its attorney fees incurred in defending itself. For still other causes of action, the answer lies somewhere in the middle, and the host will need to follow very specific procedures prescribed by statute if it wishes to avoid liability.

You can, however, take some immediate comfort in a common theme that emerges from the statutes and case law: Ignorance is bliss. Until you have some reason to believe that there is something objectionable about a Web site, courts generally will not hold liable a party that merely hosts a Web site for the same flat fee that it charges every other site. Once the host is put on notice that the site contains troublesome material, however, then the host may need to take affirmative steps to avoid liability. This article will look at some of the complaints that might be asserted and suggests steps that hosts can take to reduce their risks of liability in those different situations.

Looking at this same situation from the opposite end of the table, you might be the person who believes that a Web site is infringing your client's intellectual property or otherwise harming your client and therefore wants to shut down the site. Often the owner of an offending site cannot be identified or reached easily, but the host is readily identified. Therefore, you may want to exert pressure on the host to take down the offending site by threatening to sue the host. This article will help explain when and how you can legitimately pressure the host into taking down the site in question and when you would be well advised to either ask nicely or simply leave the host alone.

**Joel Voelzke** is a partner with the law firm of Oppenheimer Wolff & Donnelly, LLP, in Los Angeles, CA, specializing in intellectual property and Internet law. He can be reached at (310) 788-5000 and *jvoelzke@oppenheimer.com*. The views expressed herein are those solely of the author and do not reflect the views of Oppenheimer Wolff & Donnelly, LLP, or any of its clients.

## Civil Liability

Web site hosting can give rise to liability for trademark infringement and copyright infringement but generally will not give rise to liability for defamation.

### Trademark Infringement

According to at least one federal court, a host can be liable if it knows that a site is infringing a third party's trademark but fails to take steps to stop the infringement.[1] A trademark is any "mark," usually a word, a short phrase, or a logo, that serves to identify a particular source of goods or services. Examples of trademarks are the Nike "swoosh" mark and the word GUCCI. Using a mark that is identical or confusingly similar to another's valid trademark, such that consumers are likely to be confused regarding the source of the goods or services in question, constitutes trademark infringement. A trademark need not be registered with the federal government, but federal registration creates a presumption that the trademark is valid and enforceable against others.

Suppose the Web site that you host advertises leather goods that are labeled "Gucci" products, either on the goods themselves or on the Web site. This precipitates an email from Gucci America, Inc., which owns the GUCCI trademark, informing you that the goods being sold on the site are not genuine Gucci products. The email demands that you disconnect the site.

This is exactly what happened in a federal case in New York brought by Gucci America, Inc., against an online seller that was selling jewelry falsely labeled as GUCCI jewelry and against Mindspring, which hosted the offending site.[2] Mindspring argued that it should not be held liable for merely hosting the jewelry seller's site. The court disagreed, holding that Mindspring could be held liable under the trademark doctrine of contributory infringement if it continued to provide hosting services either "(1) with knowledge of the infringement or (2) with reckless disregard as to whether the material infringed the trademark owner's rights."[3]

To reach this decision, the court analogized to the trademark statute,[4] which provides immunity against a suit for money damages to printers and publishers under certain circumstances. Specifically, it exempts from liability those who merely perform the task of printing for other parties, such as label printers or newspaper publishers, provided that the printer is an "innocent infringer or innocent violator."[5] The *Gucci America* court held that a Web site host is similar to a printer or publisher, which can only be held liable if it acted with "actual malice,"[6] that is, if it acted with "knowledge of the infringement or reckless disregard."[7] This is a high standard to meet, and the court hinted that it might be difficult for the plaintiff to prove the Web site host liable under this standard.[8] In a different context, however, at least one other court has held that a printer or publisher loses its innocent-violator defense merely by failing to conduct itself in an "objectively reasonable" manner.[9]

**The *Stratton Oakmont* decision created a perverse incentive for ISPs to not self-regulate the content on their services.**

In short, if you have no reason to believe that any site that you are merely hosting is committing trademark infringement, then you should have few worries. On the other hand, if you receive information that a site that you are hosting might be infringing another's trademark, especially if you receive a direct charge of infringement from the trademark holder, do not ignore that information. Ignoring trademark infringement occurring on a hosted site could render the host contributorily liable.

The threshold requirement for liability is that a Web site host must have some knowledge or reason to know of the infringement. In the usual case in which the host has no connection to the site other than merely hosting for a normal hosting fee a site that was created entirely by another, there would not likely be liability.

In the unusual case, however, the host might have a much closer connection to the infringing site. For example, the host might also be the Web site designer who designed the site, including placing the third party's trademark somewhere on the site. Alternatively, the host might somehow be profiting from each sale that occurs on the site. In those cases, the host has gone beyond a role that is analogous to a traditional printer or publisher and might be liable for the infringement regardless of whether the host actually knew of it.

What if the cause of action asserted were trade libel under Section 43(a) of the Lanham Act? The plaintiff would want to characterize that action as an "intellectual property" action for which the host would not enjoy immunity under the Communications Decency Act (CDA). The Web site host, on the other hand, would want to characterize the action as a libel case for which the host should enjoy full immunity under the CDA in accordance with the deliberate policy choice made by Congress.

The courts have not yet addressed the issue. The discussion in *Gucci America*[10] and other cases, however, would seem to indicate that the answer would depend

on the exact nature of the allegedly libelous speech. If it were speech with a purely communicative message, such as an angry message from a disgruntled customer, then the speech would likely receive full First Amendment protection, and the case would not be considered an intellectual property matter under the Lanham Act.[11] If, however, the speech were commercial speech, such as, "Tests prove that our batteries power a toy bunny twice as long as the competitor's batteries," then the intellectual property label would probably be more apt, and the speech would not enjoy CDA immunity.

### Defamation

Slander is a false and damaging oral statement. Libel is such a statement when it is in writing. Usually, the umbrella term "defamation" is used for simplicity and encompasses both slander and libel. Because falsity is an element of defamation, truth is a complete defense to a charge of defamation. Proving that a statement is true, however, can be very difficult. If someone complains that she is being defamed by a Web site that you are hosting, it would be a significant burden to determine whether what is posted on the Web site is true or false or somewhere in between and then to prove it in court.

### Federal Immunity for ISPs under the CDA

Fortunately, Congress granted ISPs broad immunity from tort-based lawsuits such as defamation in the Communications Decency Act of 1996.[12] To understand the ISP immunity provisions of the CDA, it is helpful to first understand the court decision that gave rise to the CDA. In *Stratton Oakmont, Inc. v. Prodigy Services Company*,[13] the plaintiffs sued Prodigy for defamatory comments made by an anonymous poster on one of Prodigy's bulletin boards. The New York Supreme Court held Prodigy to the strict liability standard normally applied to original publishers of defamatory statements, rejecting Prodigy's claims that it should be held only to the lower "knowledge" standard usually reserved for mere distributors, such as news vendors and book sellers. The New York court reasoned that Prodigy had acted more like an original publisher than a distributor because it had advertised its practice of controlling content on its service and because it actively had screened and edited messages posted on its bulletin boards.

The *Stratton Oakmont* decision, therefore, created a perverse incentive for ISPs to not self-regulate the content on their services. Any attempt to screen out offensive material could automatically turn the ISP into a "publisher," thus making the ISP as legally responsible for the offensive content as if it had been the creator of that content. Fearing that the specter of liability would deter service providers from blocking and screening offensive material and would chill providers from hosting controversial but legitimate speech, Congress enacted the CDA.

The CDA embodies a policy choice by Congress not to deter harmful online speech by imposing tort liability on companies that serve as intermediaries for other parties' potentially injurious messages. Section 230 begins by reciting several Congressional findings:

> The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity. . . . The Internet and other interactive computer services have flourished, to the benefit of all Americans with a minimum of government regulation.[14]

Section 230 also states:

> It is the policy of the United States—(1) to promote the continued development of the Internet and other interactive computer services and other interactive media; (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulations; . . [and] (4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material.

The law then provides, in pertinent part, broad immunity for ISPs against liability for defamation and similar causes of action:

> (c) Protection for "Good Samaritan" Blocking and Screening of Offensive Material
>
> (1) Treatment of Publisher or Speaker
>
> No provider or user of an interactive computer service[15] shall be treated as the publisher or speaker of any information provided by another information content provider.[16]
>
> (2) Civil Liability
>
> No provider or user of an interactive computer service shall be liable on account of—
>
> (A) any action voluntarily taken in good faith

> to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.

ISPs, including Web site hosts[17] and domain name registrars,[18] qualify as providers of interactive computer services and thus are eligible for CDA immunity. Section 230 provides that "[n]othing in this section shall be construed to limit or expand any law pertaining to intellectual property."[19] The law also states that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."[20]

The CDA therefore provides a federal immunity against state law tort claims (but not federal intellectual property law claims) brought against ISPs, such as Web site hosts, for merely hosting offending sites, regardless of whether the ISP exercises editorial and self-regulatory functions.[21] That is, an ISP does not become somehow legally responsible for the Web site content by deciding that some of the content is beyond the pale and telling the hosted client that he must tone down or remove entirely some of the content. The CDA also appears to immunize the Web host against suit by a hosted customer for telling the customer that he must remove certain offensive material or have his service disconnected.

### *Examples of ISP Immunity*

The cases affirm that, under the CDA, a Web site host will not be held liable for defamation. When someone posted a phony message on an America Online (AOL) bulletin board offering offensive T-shirts for sale and listed "Ken" as the person selling the T-shirts along with his home telephone number, the Fourth Circuit held that AOL was not liable to Ken for failing to act quickly enough to take down the phony and defamatory postings.[22] When AOL, which had paid Matt Drudge $3,000 per month to publish his *Drudge Report*, published a Drudge article accusing Clinton White House aide Sydney Blumenthal of being a wife beater, the court held that the CDA immunized AOL against suit by Blumenthal.[23]

Two teachers at San Francisco City College became irate over negative reviews of them that students had posted on a teacher review Web site. They sued the Webmaster who merely operated the teacher review site but did not author any of the content. In court, the teachers dismissed their suit under threat of sanctions for proceeding further.[24] In a similar case in New Jersey, city council members brought claims for defamation, harassment, and intentional infliction of emotional distress against a Webmaster who hosted an unofficial site called "Eye on Emerson." At the "Eye on Emerson" site, citizens anonymously posted news and comments regarding events in the Borough of Emerson. The court held that the Webmaster was immune under the CDA.[25] Another court held that online bookseller Amazon.com was immune under the CDA when reader reviews panned a book. The author had tried to do a legal end-run around the CDA by casting his lawsuit as a suit for negligence, tortious interference, and breach of contract, but the court rejected that approach.[26] Other cases have yielded similar results.[27]

**As the ISP immunity provisions of the CDA become better known, defamation suits against ISPs and Web site hosts are likely to become less common.**

These cases were more or less straightforward applications of the CDA to defamation-type lawsuits. It is not clear from the statute what other state tort claims besides defamation will be precluded, but the courts have applied the CDA to the benefit of Web site hosts and other ISPs in several other contexts. When a group of college athletes brought a lawsuit for invasion of privacy against a company that was selling videotapes secretly made from hidden video cameras located in the athletes' locker rooms and against the company that hosted the Web site on which the tapes were sold, the court held that the CDA immunized the Web site host.[28]

In *Jane Doe v. American Online, Inc.*,[29] several small boys were lured into having their photographs taken while engaging in sexual activities. When the mother of one of the boys discovered that an AOL chat room was being used to sell the photographs, although the chat room was not being used to transmit the photographs, she complained to AOL. AOL did nothing in response. The mother sued AOL, claiming that AOL negligently had allowed its chat room to be used to sell child pornography, essentially asking the court to create a new tort of negligent hosting. By a bare 4-3 majority, the Florida Supreme Court held that the CDA's immunity against distributor liability applied and barred the mother's state law tort suit. Similarly, a federal court held that a registrar is immune from defamation suits based on allegedly negligent maintenance of the WHOIS database.[30]

As the ISP immunity provisions of the CDA become better known, defamation suits against ISPs and Web

site hosts are likely to become less common. Becoming more common, however, are suits in which an individual or company sues "John Doe" as the anonymous poster of an offensive message or messages and serves a subpoena on the ISP demanding that the ISP disclose the identity of the John Doe who posted the message. In one famous case, a customer who had used the online handle Aquacool 2000 sued Yahoo!, claiming that Yahoo! should have given him notice before simply "rolling over" and turning over his personal subscriber information to the plaintiff.[31] Since then, a number of ISPs have developed an unofficial policy of notifying customers that someone has subpoenaed their identification before releasing the information. The purpose of giving customers advance notice is to give them time to hire a lawyer and fight the subpoena anonymously in court if they choose to do so before responding to the subpoena. Given the current state of the law, this policy seems both reasonable and fair to subscribers.

On the other hand, a Web site host probably should not guarantee to its subscribers that it will give them advance notice. In such a case, the host's terms of use would need to include complex provisions dealing with different kinds of subpoenas, different subpoena procedures in the 50 states, and confidential subpoenas in criminal cases that may prohibit giving notice.

### *Anti-SLAPP Laws*

If a party files a lawsuit against a Web site host in connection with an allegedly defamatory Web site, the CDA provides immunity to the innocent host, and state "anti-SLAPP" statutes might require the plaintiff to pay the host's attorney fees. SLAPP is an acronym for "strategic lawsuit against public participation." Anti-SLAPP laws represent a legislative response to lawsuits, usually by large corporations, against parties for doing nothing more than exercising free speech rights. For example, when community groups would try to organize and block a developer's permits, the developer might sue, claiming that the group had conspired to interfere with the developer's business. Even though the developer might ultimately lose, the suit would force the citizens' group to spend time and significant legal fees defending itself. Such tactics threatened to chill citizens' rights to speak freely and to petition the government for redress of grievances, rights that are guaranteed by the First Amendment. Anti-SLAPP statutes protect citizens against such intimidation tactics. Many states, including California, have special anti-SLAPP statutes.

Under the California anti-SLAPP statute,[32] when a plaintiff files a lawsuit that "aris[es] from a person's act in furtherance of his rights of petition or free speech . . . in connection with a public issue," the defendant can bring a special motion to strike,[33] called an anti-SLAPP motion. In response, the plaintiff must show that he is likely to prevail on the merits of the suit. If the plaintiff fails to make that showing, then the court must dismiss the suit and order the plaintiff to pay the defendants' costs and attorney's fees.[34] The statute therefore gives defendants a tool for quickly disposing of meritless lawsuits without having to endure protracted and expensive litigation.

**If someone threatens or attempts to sue you as the host of an allegedly defamatory Web site, consider not only the substantive immunity under the CDA but also the additional advantages that may arise under a state anti-SLAPP statute.**

The statute defines an "act in furtherance of a person's right of petition or free speech" to include "any written or oral statement or writing made in a place open to the public or a public forum in connection with an issue of public interest."[35] Because the Internet is a public forum, statements posted on the Internet are eligible for protection under this statute.[36] In the teacher review Web site case mentioned earlier, when the defendant Web site operator filed an anti-SLAPP motion, the plaintiff not only dismissed the case but also agreed to pay part of the defendant's attorney fees.[37] In another case, a company sued an individual for posting certain messages highly critical of the company on investor Web sites, and the individual recovered his attorney fees when he made a successful anti-SLAPP motion to have part of the lawsuit dismissed.[38]

Therefore, if someone threatens or attempts to sue you as the host of an allegedly defamatory Web site, consider not only the substantive immunity under the CDA but also the additional advantages that may arise under a state anti-SLAPP statute.

### *Copyright Infringement*

Before the Digital Millennium Copyright Act (DMCA),[39] the case law was not entirely clear on when a host could be held liable for copyright infringement occurring on a hosted site. The general rules were that a host might be held liable if: (1) the host knew or should have known that the Web site content was infringing but failed to remove the infringing content or disable the site in a reasonably timely manner; (2) the host monitored, controlled, or had the ability to monitor or control the Web site content but had failed to

exercise that control in a reasonable manner; or (3) the host was compensated in a way that gave the host a direct financial benefit from the infringement.[40] Some of the cases leaned in the direction of making Web hosts strictly liable for copyright infringement, however.[41]

The DMCA did not change traditional copyright law as it applies to the Internet.[42] Rather, it gave to ISPs, including Web site hosts, a number of safe harbors for avoiding monetary copyright liability if the ISP follows the DMCA rules, timetables, and procedures. By implication, the DMCA gives aggrieved copyright owners a tool to help shut down infringing Web sites quickly without the Web site host or other ISP getting caught in the middle of a battle between the claimed copyright owner and the alleged infringer. Among the different safe harbors that are provided in the DMCA, the one that most directly addresses Web site host liability is Section 512(c).[43] That section addresses the liability of a computer system owner or operator when a user places infringing content on the system.

### Termination Policy and Designation of Agent

In order to even be eligible for the safe harbor protections provided in the DMCA, the service provider must meet at least four prerequisites. First, it must have reasonably adopted and implemented a policy that informs subscribers or account holders that the service provider will terminate in appropriate circumstances subscribers or account holder who are repeat infringers.[44] The ISP need not show that it ever actually terminated any subscriber; it merely needs to show that it put its subscribers on notice that they face a realistic threat of having their Internet access terminated if they repeatedly violate intellectual property rights.[45] Web site hosts should therefore incorporate within their terms of use prohibitions against infringing trademarks, copyrights, or other intellectual property rights of others and inform customers that their accounts will be terminated for repeatedly making or posting unauthorized copies.[46]

Second, the service provider must have designated an agent to receive notifications of claimed copyright infringements.[47] The form for designating an agent can be downloaded at *http://www.loc.gov/copyright/onlinesp/agent.pdf* and must be mailed, with a fee, to the Register of Copyrights. The same information also must be posted on the ISP's Web site in a place that is accessible to the public.[48] Many ISPs designate a special email address for receiving DMCA notifications, such as *dmca@Webhost.com* or *copyright@Webhost.com*. To confirm that an agent designation has been received and placed on file at the Copyright Office or to look up the designated agent for a particular entity, the public can view the Copyright Office's list of designated agents at *http://www.loc.gov/copyright/onlinesp/list/*.

Third, the service provider must not "receive a financial benefit directly from the infringing activity."[49] A direct financial benefit exists when the availability of infringing material acts as a significant draw for customers.[50] A regular Web site hosting service would easily qualify as not receiving a direct financial benefit and is the type of service that Congress meant to protect.[51] On the other hand, a company that has a more direct financial interest might not qualify. Napster, Inc., did not qualify because infringing music files were a significant draw to its service.[52]

**The ISP need not show that it ever actually terminated any subscriber; it merely needs to show that it put its subscribers on notice that they face a realistic threat of having their Internet access terminated**

Fourth, the ISP must not have actual knowledge that the material or an activity using the material is infringing53 or be aware of facts or circumstances from which the infringing activity is apparent.54

**Notification from the Copyright Owner.** An aggrieved copyright owner begins the DMCA notice-and-take-down process by sending to the service provider's designated agent a notification that "substantially complies" with the following requirements: (1) an electronic or physical signature of the person authorized to act on behalf of the owner of the copyright or other intellectual property interest; (2) identification of the copyrighted work that is claimed to be infringed; (3) identification of the material that is claimed to be infringing and information reasonably sufficient to permit the service provider to locate the material; (4) the address, telephone number, and email address of the complaining party; (5) a statement by the complaining party that he/she has a good faith belief that the disputed use is not authorized by the copyright owner, its agent, or the law; and (6) a statement by the complaining party that the information in the notice is accurate and, under penalty of perjury, that the complaining party is authorized to act on the copyright owner's or licensee's behalf.[55] The copyright owner must comply only substantially,[56] not perfectly, with the notice requirements. If the notice substantially complies with only certain of those requirements, then the ISP must promptly attempt to contact the notifier to obtain the rest of the information.[57]

A court held that Internet auction house eBay was not liable for sales of counterfeit DVDs that had occurred on eBay because the plaintiff's notice had failed to substantially comply with the DMCA's written notice requirements. Specifically, the court ruled that the plaintiff's failure to include a statement that it had a good faith belief that the works were infringed and a statement under penalty of perjury that it was the copyright owner or the owner's agent was fatal to the plaintiff's claim against eBay.[58] The court held further that the plaintiff had not given eBay enough *written* information for eBay to determine which auctions were offering bootleg copies of the movie and which were offering genuine authorized copies.[59] Consequently, the plaintiff's oral and written notices to eBay did not trigger any duty by eBay to take down the infringing content.[60] According to the court, eBay also did not have the "right and ability to control" the infringing activity within the meaning of the DMCA; the right and ability to control must mean something more than the mere ability to disable an infringing auction.[61] Although the DMCA by its own terms merely gives ISPs a safe harbor and did not otherwise change traditional copyright liability principles, the court inexplicably seemed to interpret the DMCA as providing the exclusive means by which an ISP could be held contributorily liable.[62]

**Take Down.** After receiving the notice from the copyright owner, or otherwise learning that the material in question infringes the copyrights of another, the service provider must act expeditiously to remove or disable access to the material.[63] The statute does not define "expeditiously."

The Web site owner may feel aggrieved that his site has been partly or completely disabled by an ISP. The DMCA provides immunity to an ISP that acts in good faith in disabling a site or removing allegedly infringing material from the site, however. The DMCA also exempts from liability the ISP that acts based on facts or circumstances from which infringement is apparent,[64] takes reasonable steps to promptly notify the service subscriber that it has removed or disabled access to the material on the Web site,[65] and complies with the counter-notification and reinstatement procedures described next.

**Counter-Notification and Reinstatement.** Once the ISP has notified the Web site owner that content on the site has been removed or disabled, the site owner can send a counter-notification to the ISP asking that the content be reinstated. The counter-notification must substantially include: (1) a physical or electronic signature; (2) an identification of the material removed and of its former location on the site; (3) a statement under penalty of perjury that the subscriber has a good faith belief that the material was mistakenly removed or disabled; (4) the subscriber's name, address, and telephone number; and (5) certain statements of consent to legal jurisdiction and service of process.[66] The ISP then must send a copy of the counter-notification to the person who sent the original notice and notify that person that it will reinstate the Web site content in 10 business days.[67] The ISP may reinstate the content within 10 to 14 business days following receipt of the counter-notice, unless the complaining party sends notice to the ISP that it has filed a lawsuit seeking to restrain the Web site operator from infringing.[68]

To summarize, a Web site host that wishes to avail itself of the safe harbor protections of the DMCA should:

1. Make sure that its Web site hosting policy and contracts advise customers that their service may be terminated if they are repeat infringers of others' rights.

2. Designate an agent to receive notice of alleged copyright infringement, file the designation with the copyright office, post the designation on the host's Web site, and make sure that the agent designation remains accurate and up-to-date.[69]

3. If the host receives notice of alleged copyright infringement, it should act quickly in accordance with the procedures and timetables set forth in the DMCA. If the host does not follow the procedures necessary to take advantage of the DMCA safe harbor, the host's liability will likely be determined under traditional copyright principles.[70] That law generally favors a completely innocent ISP but nevertheless poses certain dangers for ISPs.

## Criminal Liability

There are few reported cases in the United States of a Web site host's being criminally prosecuted for merely hosting or allowing access to a Web site or other online content. A Web site host conceivably could be criminally liable for the content of a Web site on several different theories, however; hosts should be aware of those theories to help avoid trouble. First, there are some statutes that place an affirmative duty on persons to police the use to which their facilities or services are put, at least after having been notified of the wrongful use of those facilities. Second, knowingly possessing certain electronic material can be a crime, and the Web site host could be considered to possess those files by

virtue of the files' being stored on its servers. Third, a person who knowingly helps to carry out crimes, and who does so with the purpose and intent that the crimes can be committed, can be prosecuted as an aider and abetter of the crime under traditional principles of criminal law.[71]

As a general rule, therefore, a hosting contract should prohibit illegal activity on the site and give the host the right to suspend or terminate service if it believes that the Web site contains illegal material, is being used in an illegal way, or would otherwise subject the host to criminal liability.

**Under 42 U.S.C. § 13032(b), the ISP does not have any duty to monitor its network. In addition, ISPs are immune from civil suits for acts taken in good faith to comply with the law.**

Recognizing the difficulties and chaos that could result from holding Web site hosts criminally liable for content posted by others on the hosted sites, several bills have been introduced in Congress that would grant immunity from criminal prosecution for merely hosting Web sites. H.R. 3716, introduced by Senator Robert Goodlatte (R-Va.), would clarify that ISPs cannot be held criminally liable for any acts by third parties, as long as the ISP did not intend to facilitate any crime. Although some states have passed laws giving ISPs at least limited immunity,[72] as of this writing none of the federal bills have become law. Given the dearth of cases holding ISPs criminally liable and the sound reasons for not doing so except in the most egregious circumstances, Web site hosts have little to worry about in most cases and need not actively seek out problematic sites.

### Child Pornography

Under 42 U.S.C. § 13032(b), an ISP that learns that its services are being used to transmit child pornography must report the relevant facts as soon as reasonably possible to agencies designated by the US Attorney General to receive such reports. Violators can be fined up to $100,000.[73] The ISP does not have any duty to monitor its network,[74] however. In addition, ISPs are immune from civil suits for acts taken in good faith to comply with the law.[75]

A different statute, 18 U.S.C. § 2252(a), prohibits knowingly receiving, possessing, distributing, reproducing in commerce, or transporting by any means including a computer visual depictions of a minor engaged in sexually explicit conduct. Arguably, a Web site host that knows that the hosted site contains or is being used to store or transmit banned material falls within the wording of the child pornography statute and could be subject to prosecution if it does not shut down the site.

Note that these two federal statutes taken together could create a potential Catch-22 for Web site hosts. If the host learns that child pornography is being transmitted through its network, it must make a 42 U.S.C. § 13032(b) report to law enforcement of that fact. At the same time, the mere reporting will establish a *prima facie* case that the ISP knew that its network was being used to send child pornography, thus exposing the ISP to a charge under 18 U.S.C. § 2252(a) of *knowingly* possessing or distributing child pornography.

Until Congress passes a law that sets a clearer national standard for when Web site hosts can be criminally liable for Internet content produced by others and merely residing on or sent through their systems, state law will at least partially control. Different states have taken different approaches to whether an ISP should be held liable for child pornography on the Internet. Law enforcement officials in New York threatened ISP BuffNET with criminal liability for failing to block its subscribers from accessing a newsgroup that was being used to disseminate child pornography. The ISP eventually pleaded guilty to the crime of criminal facilitation, a misdemeanor.[76] According to the NY Attorney General, the BuffNET plea established that, "[w]hen . . . any ISP is informed of this kind of heinous criminal activity, it has a duty to act."[77]

New York's aggressive position—threatening ISPs with criminal liability for failing to prevent subscribers from accessing information available on the Internet—runs somewhat counter to the *Jane Doe v. American Online, Inc.*, case.[78] Thus, while Web site hosts appear to be immune from civil suits under the CDA and the *Jane Doe* case for not blocking access to child pornography, the hosts still can be threatened with criminal prosecution at the federal and state levels.

Pennsylvania passed a law, H.B. 1333, which holds ISPs criminally liable for failing to block child pornography on the Internet once the ISP has been formally notified that its service is being used to transmit child pornography.[79] Under the law, which took effect in April 2002, ISPs are not required to monitor the Internet but need act only when notified of the problem. The state first obtains a court order declaring certain material to constitute probable cause evidence of a violation of Pennsylvania's child protection laws. The state then notifies the ISP of the court order, and the ISP then must not only take down child pornography on the parts of the system that it controls but also must block specific sites or services. ISPs that fail to comply

will be subject to penalties of $5,000 for a first offense and up to $30,000 plus seven years in prison for repeat offenses.

The state of Virginia took a much different approach and granted to ISPs and email providers statutory immunity for obscene content that may be harmful to minors when the ISPs are merely passive conduits for the pornography.[80] South Dakota, on the other hand, requires ISPs to report any child pornography to law enforcement officials.[81]

### Gambling

Currently, the legality of gambling on the Internet is being debated and legislated in numerous states. Nevertheless, a federal law requires that a "common carrier, subject to the jurisdiction of the Federal Communication Commission" deny service to any customer who is using the facilities to transmit gambling information after a law enforcement agency has notified the carrier in writing that the customer is using the facilities in that way and after reasonable notice to the customer.[82] The carrier is not liable to the customer for terminating service under those conditions.[83] A Web site host might fall within this statute. Consequently, a host that receives notice from a law enforcement agency under this section, stating that a hosted Web site is being used to conduct illegal gambling over the Internet, may be required to terminate the site.

The NY Attorney General has begun pressuring financial service providers, such as credit card issuers, to stop allowing their services to be used to pay for online gambling. The Attorney General is applying the same "facilitation" rationale in the gambling context as he used to prosecute BuffNet for facilitating child pornography.[84] Therefore, Web site hosts could find themselves the target of criminal prosecutions for hosting or allowing access to online gambling or any other illegal activity. Whether such criminal charges would withstand a court challenge remains to be seen.

### Cross-Border Issues

Merely avoiding liability under US law might not be enough. A foreign court might decide that a US-based Web site violates the laws of that country and order the Web site shut down or attempt to impose civil or criminal liability on the host. Foreign countries have begun holding their own ISPs criminally responsible for the content on their systems in some cases.[85] Whether foreign courts will attempt to hold ISPs located in other countries responsible for the content on their systems and how foreign governments will attempt to enforce those laws across international borders, is only beginning to be tested. It is clear, however, that foreign courts have begun attempting to hold US Web site operators liable.

The High Court of Australia recently asserted jurisdiction over the operators of the *Wall Street Journal* site (*www.wsj.com*) on the ground that an article posted there defamed an Australian citizen and therefore caused harm in that country.[86] A French judge ordered a Web site host, SkyNet WEB Ltd., to report what actions it would take to block access to a racist Web site hosted by front14.org.[87] The court's order was based on article 24 of the law of July 29, 1881, on freedom of the press, which prohibits inciting discrimination, hatred, or violence based on race.

**The NY Attorney General has begun pressuring financial service providers to stop allowing their services to be used to pay for online gambling.**

In an unrelated but similar case, however, a US judge held that French law prohibiting the sale of Nazi memorabilia could not be given legal effect against Yahoo! in the United States because the First Amendment precludes enforcement within the United States of a French order intended to regulate the content of Yahoo!, Inc.'s speech over the Internet.[88] Nevertheless, the French court asserted jurisdiction over Yahoo! and its former CEO Timothy Koogle. The court eventually found in favor of Yahoo! and Koogle on substantive rather than jurisdictional grounds.[89]

In sum, it is possible that a US-based Web site host could be held liable for violating the laws of a foreign country, and a criminal judgment might conceivably be enforceable in the United States when the foreign law does not conflict with any US law. Whether and under what circumstances a host can be held liable in another country for the content of a hosted site will probably remain the subject of international debate for a long time.

### Conclusions: What Hosts Should Do Now

In conclusion, if you are a Web site host, there are several things you can do now to reduce your chances of being caught in the legal crossfire between a hosted client and an aggrieved third party.

First, designate an agent to receive notice of copyright infringement under the DMCA. File the designation of agent form in the US Copyright Office, post the agent's contact information in an appropriate place on your Web site, and keep the information up to date.

In addition, the hosting contract should include provisions similar to the following, either explicitly in the contract or by incorporating by reference the host company's terms of service:

- The client will not commit any criminal or tortious activity through the use of the service, including trademark infringement, copyright infringement, patent infringement, theft of trade secrets, fraud, child pornography, trafficking in obscene material, violation of US export restrictions, drug dealing, gambling, harassment, stalking, spamming,[90] hacking, sending of viruses or other harmful files, or illegal posting of computer passwords or computer code, for the purpose of circumventing copyright security measures.
- Repeat violators will be terminated.
- You reserve the right to terminate service if, in your sole discretion and judgment, the client's Web site or use of your service may result in civil or criminal liability to you.
- The client agrees to indemnify you if the client's Web site or use of your service causes you to be held civilly or criminally liable to another.
- You will comply with all subpoenas and court orders that appear to be lawful and valid, including subpoenas and court orders requesting information about the client and his use of the service.
- You reserve the right to report potentially criminal activity to appropriate law enforcement agencies.
- If the client's server is involved in an attack on any computer system, either with or without the client's knowledge or complicity, the server will be shut down while the problem is being investigated and fixed.
- The contract should include a designation by both the client and you of addresses and email addresses for the sending of notifications under the DMCA.

Additionally, if you do receive a cease-and-desist notice from a party claiming that the site you are hosting violates its rights, consider the matter carefully. If the party complains about being defamed, the potential for liability is minimal because the CDA gives broad immunity to merely passive Web site hosts. On the other hand, if the person complains of trademark or copyright infringement, then you will probably need to perform at least some investigation and/or take some responsive action. If the person is complaining about copyright infringement and has a complaint that you cannot determine is meritless, be sure to carefully follow the notice-and-take-down procedures and timetables in the DMCA in order to avail yourself of the DMCA's safe harbor for ISPs. By taking the above steps now and by seeking the advice of an attorney who keeps abreast of this fast-changing area of law if and when you receive a complaint, you should be able to remain an innocent Web site host in the eyes of the law.

## Notes

1. Gucci Am., Inc. v. Hall & Assoc., 135 F. Supp. 2d 409 (S.D.N.Y. 2001).
2. *Id.*
3. *Id.* at 420, 422.
4. 15 U.S.C. § 1114(2)(A), (B).
5. *Id.*
6. *Gucci*, 135 F. Supp. 2d at 420, 422.
7. *Id.*
8. "[T]rademark plaintiffs bear a high burden in establishing 'knowledge' of contributory infringement." *Id.* at 420.
9. Dial One of the Mid-South Inc. v. Bellsouth Telecomm., Inc., 269 F.3d 523, 526 (5th Cir. 2001). In this case, the defendant was a printer of a yellow pages telephone directory. The plaintiff notified the defendant that a franchisee had been terminated and therefore should no longer be listed in the yellow pages as a licensed franchisee. The publisher left the yellow pages listing unchanged. The jury found the publisher liable for trademark infringement for falsely identifying the terminated entity as a licensed franchisee, and the Court of Appeals for the Fifth Circuit let the award stand, ruling that there was sufficient evidence for the jury to conclude that the printer had failed to act in an objectively reasonably manner.
10. *See Gucci*, 135 F. Supp. at 415-418.
11. *Cf.* Scotts Co. v. United Indus. Corp., No. 02-1738 (4th Cir., Dec. 22, 2002) (holding that employee comments disparaging a competitor's products do not qualify as "commercial advertising and promotion" because those comments were not intended to influence consumer purchasing decisions and were not widely disseminated and therefore do not give rise to a Lanham Act claim for false advertising). *See also* Taubman Co. v. Webfeats, No. 03a0043 (6th Cir. Feb. 7, 2003) (holding that the "gripe site" *www.taubmansucks.com* was entitled to First Amendment protection against prior restraint of speech).
12. 47 U.S.C. § 230.
13. Stratton Oakmont, Inc. v. Prodigy Services Company, 1995 N.Y. Misc. LEXIS 229, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).
14. 17 U.S.C. § 230(a)(4), (5).
15. An "interactive computer service" means "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." 47 U.S.C. § 230(f)(2).
16. An "information content provider" means "any person or entity that is responsible, in whole or in part, for the creation or

development of information provided through the Internet or any other interactive computer service." 47 U.S.C. § 230(f)(3).

17. *Cf.* Hendrickson v. eBay Inc., 165 F. Supp. 2d 1082, 1088 (C.D. Cal. 2001) (holding that Internet auction house eBay easily qualifies under the broad definition of an Internet "service provider" under the DMCA).
18. *E.g.*, Greg Lloyd Smith v. Intercosmos Media Group, No. 02-1964, 2002 U.S. Dist. LEXIS 24251 (E.D. La. Dec. 17, 2002).
19. 47 U.S.C. § 230(e)(2).
20. 47 U.S.C. § 230(e)(3).
21. Zeran v. America Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997).
22. *Id.*. Although the plaintiff attempted to cast his lawsuit not as a defamation action *per se*, but as a negligence action for AOL's conduct in not removing the offending content quickly enough, the court disagreed and treated the lawsuit as "indistinguishable from a garden variety defamation action." *Id.* at 332.
23. Blumenthal v. Drudge, 992 F. Supp. 44, 53 (D.C. 1998).
24. *See* ACLU press release, *In Free Speech Victory, City College Teachers Agree to Dismiss Lawsuit Against Critique Web Site*, Oct. 3, 2000, at *http://www.aclu.org/news/2000/n100300a.html* (on file with the author).
25. Donato v. Moldow, Docket No. BER-L-6214-01, at *http://www.geocities.com/emersoneye/lawsuit/decision.html* (on file with the author).
26. Schneider v. Amazon.com, Inc., 108 Wash. App. 454, 311 P.3d 37, 29 Media L. Rep. 2421 (Wash. Ct. App. 2001).
27. *See, e.g.*, Jane Doe One v. Oliver, 46 Conn. Supp. 406, 755 A.2d 1000 (Conn. Sup. Ct. 2000).
28. John Does 1 through 30 v. Franco Prods., 2000 U.S. Dist. LEXIS 8645 (N.D. Ill. June 21, 2000).
29. Jane Doe v. American Online, Inc., 783 So. 2d 1010 (Fla. 2001).
30. Greg Lloyd Smith v. Intercosmos Media Group, No. 02-1964, 2002 U.S. Dist. LEXIS 24251 (E.D. La. Dec. 17, 2002).
31. *See* "Suit Raises Rights of Internet Users when ISPs are Subpoenaed for Personal Information," at *http://www.techlawjournal.com/privacy/20000514.htm* (on file with the author), reporting on *John Doe aka Aquacool_2000 vs. Yahoo! Inc.*, filed in the Central District of California in 2000.
32. Cal. Code Civ. P. § 425.16.
33. *Id.* § 425.16(b).
34. *Id.* § 425.16(c).
35. *Id.* § 425.16(e)(3).
36. ComputerXpress, Inc. v. Jackson, 93 Cal. App. 4th 993, 1007 (2001).
37. *See* ACLU press release, *supra* note 24.
38. *ComputerXpress*, 993 Cal. App. 4th at 1020.
39. 17 U.S.C. § 512.
40. *See, e.g.*, Marobie-FL, Inc. v. National Ass'n of Fire Equip. Distribs., 983 F. Supp. 2d 1167 (N.D. Ill. 1997); Religious Technology Center v. Netcom On-Line Comm. Servs., Inc., 907 F. Supp. 1361, 1373-1374 (N.D. Cal. 1955) ("If plaintiffs can prove the knowledge element, Netcom will be liable for contributory infringement since its failure to simply cancel Erlich's infringing message and thereby stop an infringing copy from being distributed worldwide constitutes substantial participation in Erlich's public distribution of the message."); Ellison v. Robertson, 189 F. Supp. 2d 1051, 1057-1064, (C.D. Cal. 2002).
41. *See* Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993); Central Point Software, Inc. v. Nugent, 903 F. Supp. 1057 (E.D. Tex. 1995); Playboy Enters., Inc. v. Webbworld, Inc., 991 F. Supp. 2d 543 (N.D. Tex. 1997).
42. *Ellison*, 189 F. Supp. 2d at 1061 (citing legislative history of the DMCA, H.R. Rep. 105-551(II), at p. 64 (July 26, 1998)). *But see* Hendrickson v. eBay, *infra* note 62.
43. 17 U.S.C. § 512(c); *Ellison*, 189 F. Supp. 2d at 1068.
44. 17 U.S.C. § 512(i)(1).
45. *Ellison*, 189 F. Supp. at 1065 (citing legislative history of the DMCA, H.R. Rep. 105-551(II), at p. 61 (July 26, 1998)).
46. *See id.* at 1056 (citing AOL's terms of service as sufficient evidence that AOL complied with the reasonable termination policy prong of the safe harbor provisions of 17 U.S.C. § 512(a)).
47. 17 U.S.C. § 512(c)(2).
48. *Id.*
49. *Id.* § 512(c)(1)(B).
50. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001).
51. *Ellison*, 189 F. Supp. 2d at 1062-1064.
52. *Napster*, 239 F.3d at 1023 ("Financial benefit exists where the availability of the infringing material acts as a 'draw' for customers.") (quoting Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 257, 263-264 (9th Cir. 1996)).
53. 17 U.S.C. § 512(c)(1)(A)(i).
54. *Id.* § 512(c)(1)(A)(ii).
55. *Id.* § 512(c)(3).
56. *Id.* § 512(c)(3)(A), (B).
57. *Id.* § 512(c)(3)(B)(ii).
58. Hendrickson v. eBay Inc., 165 F. Supp. 2d 1082, 1090-1092 (C.D. Cal. 2001).
59. *Id.* at 1093. *Compare* ALS Scan v. Remarq Cmtys., Inc., 239 F.3d 619, 625 (4th Cir. 2001) (copyright owner substantially complied with DMCA notification requirements when owner provided ISP with information that identified two newsgroups as being created solely for the purpose of distributing unauthorized copies of its copyrighted works, asserted that virtually all the images at the two sites were its copyrighted material, and referred the ISP to two Web addresses where the ISP could find pictures of its models and obtain copyright information).
60. *Hendrickson*, 165 F. Supp. 2d at 1092.
61. *Id.* at 1094. *Accord*, *Ellison*, 189 F. Supp. 2d at 1062.
62. The court seemed to ignore the fact that eBay might still be liable for contributory infringement under traditional principles of contributory infringement. According to the court, the

plaintiff had never provided *written* notice to eBay as to which auctions infringed; therefore, the court could simply ignore evidence that the plaintiff had told eBay via telephone specifically which items infringed. *Hendrickson,* 165 F. Supp. 2d at 1091-1092 n.8, n.10, 1093. Under traditional contributory infringement principles, there is no reason that oral notice would have been insufficient to put eBay on clear enough notice to trigger contributory liability.

63. 17 U.S.C. § 512(c)(1).
64. *Id.* § 512(g)(1).
65. *Id.* § 512(g)(2)(A).
66. *Id.* § 512(g)(3).
67. *Id.* § 512(g)(2)(B).
68. *Id.* § 512(g)(2)(C).
69. In *Ellison,* AOL had designated an agent but inexplicably failed to notify the copyright office for several months that it had changed its email address for receiving DMCA infringement notices. Author Harlan Ellison's lawyer sent an email to AOL advising it of infringement of Ellison's books on AOL's usenet groups. AOL claimed, however, to have never received the notice because notice was sent to the old email address. The court decided that it was AOL's own fault that it did not receive the lawyer's notice, and therefore a jury could find that AOL should have known of the infringement even though it did not actually know of the infringement. 189 F. Supp. 2d at 1057-1058.
70. *See, e.g., ALS Scan,* 239 F.3d at 626.
71. *See, e.g.,* 17 Cal. Jur. 3d, Criminal Law § 105 (Bancroft-Whitney 1984).
72. *E.g.,*Va. Code Ann. § 18.2-391 (exempting ISPs from a Virginia state law that prohibits the knowing display of sexually explicit materials used for a commercial purpose that may be harmful to juveniles), as explained in PSINET, Inc. v. Chapman, 108 F. Supp. 2d 611 (W.D. Va. 2000).
73. 42 U.S.C. § 13032(b)(3)(B).
74. *Id.* § 13032(e).
75. *Id.*§ 13032(c).
76. *See* New York Attorney General Press Release, "Breakthrough Cited in War Against Child Porn: Internet Service Provider Forced to Acknowledge Obligations to Terminate Illegal Activities," Feb. 16, 2001, available at *http://www.oag.state.ny.us/press/2001/feb/feb16c_01.html* (on file with the author).
77. *Id.*
78. Jane Doe v. American Online, 783 So. 2d 101029.
79. Computer Technology Law Report, BNA, Inc. Vol. 3, No. 7, April 5, 2002, at 125. *See http://www.legis.state.pa.us/WU01/LI/BI/BT/2001/0/HB1333P3184.HTM* for the text of the bill.
80. *See* PSINET, Inc. v. Chapman, 108 F. Supp. 2d 611 (W.D. Va. 2000) (applying Va. Code Ann. § 18.2-391).
81. "Pa. Law: ISPs Must Block Child Porn," available at *http://news.findlaw.com/ap/ht/1700/3-18-2002/20020318101648 6709.html* (on file with the author).
82. 18 U.S.C. § 1084(d).
83. *Id.*
84. Based on conversations between the author and representatives of the NY Attorney General's office.
85. North Korea police indicted three executives of the North Korean portal site "N," which operated a "photo album" service. According to the charge, the executives neglected their duties under North Korean law to monitor the photos posted by users to the site to ensure that obscene material was not posted and to ensure that the site was not being improperly accessed by minors. *See* "Portal Webmasters Indicted for Failing to Stop Pornography," available at *http://www.chosun.com/w21data/html/news/200204/200204041021.html* (on file with the author).
86. Dow Jones & Company Inc. v. Gutnick, [2002] HCA 56 (10 Dec. 2002), available at *http://www.austlii.edu.au/au/cases/cth/high_ct/2002/56.html.*
87. Catherine Muyl, "Cross-Border Public Policy Internet Issues," *Intellectual Property Today,* Mar. 2002, 22, 23.
88. Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 169 F. Supp. 2d 1181, 1193 (N.D. Cal. 2001).
89. *See* "Ex-Yahoo Chief Acquitted over Nazi Relics," Feb. 11, 2003, available at *http://news.com.com/2100-1023-984148.html* (on file with the author).
90. A NY court recently held that ISP PaeTec could drop MonsterHut as a client due to MonsterHut's violation of PaeTec's anti-spam policy. MonsterHut, Inc. v. PaeTec Comm. Inc., No. CA 01-02396 (N.Y. Sup. Ct., Appellate Div., May 3, 2002).