New Media, Information Technology, & Online Law

The COMPUTER Lawyer

Volume 17 ▲ Number 2 ▲ FEBRUARY 2000

Features

Current Developments

Note: The 21st Annual USC Computer & Internet Law Institute is May 11–12. For details, see Back Cover.

Edited by Blanc Williams Johnston & Kronstadt LLP, Los Angeles, CA

Aspen Law & Business

New Cybersquatting Law Gives Trademark Owners Powerful New Weapons Against Domain Name Pirates

by Joel Voelzke

On November 29, 1999, President Clinton signed into law an omnibus budget bill that included significant new intellectual property provisions, including the Anticybersquatting Consumer Protection Act (the Act). The Act articulates a strong federal policy against registering or keeping domain names for the main purpose of profiting by selling those domain names to trademark owners or to people whose personal names are similar to the domain name. Under the new law, it will be much easier for a plaintiff to take action against the owner of a domain name that corresponds to his or her trademark or personal name, and to obtain an order canceling or transferring the domain name. The new law also gives a trademark owner the option to proceed *in rem* against the domain name itself, remedying the previous difficulties raised by domain name registrants who could not be located. Additionally, domain name registrars such as Network Solutions, Inc. will enjoy immunity from suit with respect to the "reasonable" registering, suspending, canceling, or transferring domain names.

This article examines the text and impact of the new law. In the discussion that follows, statutory citations are according to where the Act will be codified, if specified. The article also describes some of the steps companies should now consider with their counsel to protect themselves and their trademarks.

Liability Standard

Liability Standard in General: "Bad Faith" Is the Key

The Act protects owners of both registered and unregistered trademarks against use of their marks within domain names, and also protects living persons against use of their personal names within domain names, under certain circumstances. Under § 43(a) of the Lanham Act as amended by the Act, a domain name holder becomes liable if he or she:

> (i) "has a bad faith intent to profit from" a mark or personal name protected by § 43 (see below for a discussion of the "bad faith" standard), and
>
> (ii) registers, traffics in, or uses a domain name that is:
>
> (A) identical or confusingly similar to a distinctive mark;
>
> (B) identical, confusingly similar, or dilutive of a famous mark; or
>
> (C) is protected under 18 U.S.C. 706 (Red Cross) or 36 U.S.C. 220506 (Olympics and related marks).[1]

Whether the mark is distinctive or famous is to be judged at the time of registration.[2]

The "confusingly similar" standard is to be applied without regard to the respective goods and services of the parties.[3] This is an important change. Previously, a trademark owner had two primary avenues for pursuing a cybersquatter. First, the owner could try to prove that the cybersquatter was diluting the trademark. This required a showing that the trademark was "famous."[4] If the mark were not proven to be famous, the second possibility was to charge the cybersquatter with infringing the trademark. However, traditional trademark infringement analysis requires a likelihood of consumer confusion *after* taking into account how closely related the goods and services of the parties are. Because most cybersquatters do not actually sell any goods or services, there was some question as to whether trademark owners could prove infringement where the domain name was never actually used to sell goods or services. Under the new law, however, it suffices if the domain name is confusingly similar to the mark, without reference to the goods or services of the parties. Therefore, the owner of even a non-famous mark can now clearly obtain relief against a cybersquatter.

Joel Voelzke is an attorney at Oppenheimer Wolff & Donnelly LLP in Los Angeles, CA. He wishes to thank Erika Coster and Jane Shay Wald for their valuable suggestions and assistance. Email: <jvoelzke@oppenheimer.com>

Multi-Factored "Bad Faith" Test for Trademarks Used as Domain Names

At a loss as to exactly how to define "cybersquatting," Congress eschewed any bright lines for judging when the use of a domain name was wrongful. Instead, the Act directs courts to apply a multi-factored "bad faith" test. The bad faith factors include:

- whether the domain name holder has any legitimate trademark or other intellectual property rights in the domain name, or whether the domain name is the holder's own name;
- any prior use of the domain name by the holder in the *bona fide* offering of goods/services;
- the holder's intent to divert consumers from the mark owner's own site, for either commercial gain or to tarnish or disparage the mark;
- the holder's attempts to sell the domain name without a prior *bona fide* offering of or intent to offer goods/services, or the holder's past pattern of doing so;
- whether the holder supplied false or misleading contact information when applying to register the domain name, or other domain names;
- whether the holder has acquired other domain names that are the same or similar to other trademarks; and
- how distinctive or famous the mark is.[5]

Although the domain name holder's legitimate rights to use the disputed domain name within his or her own field is listed as only one factor for the court to consider, the Act goes on specifically to exclude a finding of bad faith in those cases in which the domain name holder reasonably believed that the use of the domain was a fair use or "otherwise lawful."[6] This somewhat circular definition would seem to follow the recent holding in *Hasbro Inc. v. Clue Computing Inc.*,[7] the <*clue.com*> case. The court in that case held that a smaller company that uses a domain name that incorporates a mark being used in a field that does not infringe on the larger company's mark, and who registered the disputed domain name first, has every right to use the domain name as long as it uses the domain name for legitimate commerce, and does not try to sell the domain name to the other trademark owner.

Names of Living Individuals: "Intent to Profit" Is the Test

The substantive standard for determining when the name of a person is being cyberpirated is different from the standard that applies to a trademark used as a domain name. Specifically, the Act prohibits registering a domain name that is identical or confusingly similar to the name of a living person "with the specific intent to profit from such name by selling the domain name." There is an exception for copyright owners and licensees who register a domain name in connection with a "work of authorship," where the copyright owner/licensee intends to sell the domain name "in conjunction with the lawful exploitation of the work."

Because the liability standard turns on the registrant's subjective intent, even someone coincidentally named Vanna White would run afoul of the law if she were to register her own name as a domain name with the intent to sell the domain name, either to the famous Ms. White or to a third party. Note that the Act makes no distinction between whether the person whose name is similar to the domain name is famous or not. Even ordinary people are protected against having their names cyberpirated by companies or individuals scooping up large numbers of domain names in the hopes of ransoming them back to the people who happen to have those names.

Additionally, the Act directs the Secretary of Commerce to conduct further studies and make recommendations for additional rules to prevent "abusive" registration of domain names that consist in whole or in part of personal names, including the names of government officials and candidates for public office.

Remedies and Effective Dates

Two different remedies apply depending on whether the right violated is a trademark or a right in a personal name already protected under Section 43 of the Lanham Act, or merely a person's unregisterable name.

Violations of a Trademark and Names Protected under Section 43

Monetary Remedies

For wrongful registration, trafficking, or use of a domain name that occurs *after* the enactment of the Act, plaintiffs are eligible for the same monetary remedies and injunctions as currently apply to other Lanham Act violations: (1) defendant's profits, (2) up to three times damages, (3) costs, and (4) in exceptional cases, attorney fees.[8] Additionally, the Act gives plaintiffs the option of statutory damages: At any time prior to final judgment the plaintiff can waive his or her actual dam-

ages and elect to receive statutory damages in the amount of $1,000 to $100,000 as the court deems just.[9]

Cancellation or Transfer Order

An important feature of the Act is that it specifically provides for injunctions ordering cancellation or transfer of domain names that were registered before, on, or after the Act's enactment.[10]

Violations of a Person's Name

With respect to a domain name that violates a person's name under the Act, but that does not rise to the level of an independent Section 43 violation, and was registered on or after the date of enactment, a court may award the aggrieved individual an injunction ordering cancellation or transfer of the domain name, as well as costs and attorney fees.

In Rem Proceedings

One of the most important changes is that a trademark owner can now bring an *in rem* action against the domain name itself.[11] This overturns the holding in *Porsche Cars North America Inc. v. Porsche.com*,[12] in which the court held that the Lanham Act did not authorize *in rem* actions. Under the new law, if the trademark owner cannot obtain personal jurisdiction, or if it sends notice to the holder at both the postal address and the email address listed in the registration and the registrant does not answer, the trademark owner can then proceed *in rem* against the mark itself. Sending the notice constitutes service of process.[13]

An *in rem* suit can be brought in the judicial district where the registrar is located, or where "documents sufficient to establish control and authority regarding the disposition of the registration and use of the domain are deposited with the court."[14] It would appear, therefore, that a trademark owner can bring an *in rem* action in any judicial district as long as the registrar (*i.e.*, the company which registered the domain name for the domain name holder), agrees either beforehand or after the suit has been filed to deposit the necessary documents with the court. For brevity, depositing the required documents with the court will be referred to below as depositing the domain name with the court.

One obvious advantage to proceeding *in rem* is that a domain name holder can no longer hide from the trademark owner, and the notice and service procedures are extremely simple to fulfill. An additional and important advantage is that as soon as the plaintiff gives to the registrar a file stamped copy of the complaint, the registrar must freeze the domain name (*i.e.*, the registrar must not transfer or cancel the registration except as ordered by the court).[15] The registrar must also deposit the domain name with the court.[16]

One of the most important changes is that a trademark owner can now bring an *in rem* action against the domain name itself.

The disadvantage to proceeding *in rem* is that the court can grant only injunctive relief in the form of a forfeiture, cancellation, or transfer order. Damages and attorney fees cannot be awarded. However, the *in rem* procedure is not exclusive; a trademark owner can still bring a regular civil action for damages against the domain name holder in addition to the *in rem* action against the domain name itself.[17]

If you are trademark owner, subject to the advice of your counsel it appears that the quickest and most efficient method of proceeding against a cybersquatter who cannot be readily identified and/or located, would be to:

1. Contact the registrar of the disputed domain name, and ask whether the registrar would be willing to deposit the domain name in the court of your choosing. Most registrars will probably be willing to do so. If the registrar agrees, you can file the action in the venue of your choice. If the registrar does not agree, you will have to file the action in the judicial district which is the situs of the domain name, which is defined by the Act to be the district where the registrar, registry, or other domain name authority that registered or assigned the domain name is located.
2. Send notice via mail and email to the domain name holder that you intend to file an *in rem* action against the domain name under 15 U.S.C. § 1125(d)(2).
3. File both an *in personam* action naming the putative domain name holder and Does as defendants, and an *in rem* action against the domain name.
4. Immediately deliver a file stamped copy of the complaint to the registrar. This will force the registrar to freeze the domain name, thus preventing the domain name from being sold or transferred.

Protection for the Current Domain Name Holder

What if a company accuses somebody else of cybersquatting, and the registrar suspends or cancels the disputed domain name as a result? Does the former domain name holder have a procedure for recovering the domain name? The answer is, "Yes." If a registrar suspends or transfers a domain name, the original domain name holder can then bring a civil suit presumably against the registrar, with notice to the trademark owner, seeking a judicial declaration that his or her use of the domain name was in fact lawful. If the original holder is successful, the court can issue an order that the domain name be reactivated or transferred back to the original holder.

Collect and document any explicit or implicit offers that you have received from cybersquatters to sell their domain names.

What if a domain name was canceled in response to a cybersquatting accusation that was based on a misrepresentation by the accuser? In that case, the domain name holder has an additional remedy. Anyone who makes a knowing and false representation that a domain name is identical, confusingly similar to, or dilutive of a mark, thereby inducing the registrar to take action with respect to the disputed domain name, is liable for both the domain name holder's actual damages as well a nondiscretionary award of costs and attorney fees.[18]

Provisions Affecting Domain Name Registrars

Domain name registrars such as Network Solutions, Inc. will not be monetarily liable for registering domain names unless they act with a "bad faith intent to profit" from the registrations,[19] or act in "bad faith or reckless disregard."[20]

Domain name registrars receive an additional safe harbor to encourage them to develop and implement their own policies for policing domain names. If the registrar adopts and follows a "reasonable policy" of refusing to register, removing from registration, transferring, or temporarily or permanently canceling a domain name registration, then the registrar will not be liable for damages caused by action that it takes under that policy.[21]

As mentioned above, a registrar who receives a file stamped copy of an *in rem* complaint must freeze the domain name and deposit the domain name with the court.

What Companies Should Do Now

By consulting with their counsel to take the following steps now, companies will help to strengthen their cybersquatting challenges to domain names held by others, and will help to protect their own domain names from cybersquatting challenges brought by others.

- If possible, register, or apply to register, your domain name as a trademark with the US Patent and Trademark Office.
- Document your *bona fide* selling of goods and services or your *bona fide* intention to sell goods and services using your domain name. This will help to fend off, if necessary, a challenge by another to your company's right to use that domain name or to warehouse the domain name for future use.
- Immediately identify all domain names that are owned by others but that are similar to your trademarks. Visit those cites. Print out the pages that show whether or not the domain name is being used in the *bona fide* offering of goods and services. Some cybersquatters freely admit (or even brag) on their pages that they are cybersquatters, and that they intend to sell to the highest bidder. Obtaining printouts of such pages now—before the cybersquatter can change them—will be extremely helpful in making your cybersquatting case later.
- Collect and document any explicit or implicit offers that you have received from cybersquatters to sell their domain names.
- Study the domain name dispute policy, if any, of the registrars who registered the domain names that you would like to obtain. Determine with your counsel whether you would prefer to proceed under the dispute policy including arbitration if provided for, or via court action. Ask the registrar whether it is willing to deposit the domain name in the court that you would prefer to hear the dispute.
- If applicable, have your counsel send, via US mail and email, notices to those persons who are

cybersquatting in violation of your rights, asking them to identify themselves and informing them that you intend to file an *in rem* action against the disputed domain name under the Anticybersquatting Consumer Protection Act,[22] if they do not identify themselves by a specific deadline. Once you file your *in rem* complaint, immediately deliver a file stamped copy of the complaint to the registrar, thereby forcing the registrar to freeze the domain name and deposit the domain name with the court.

Notes

1. 15 U.S.C. § 1125(d)(1)(A) (1999).
2. *Id.*
3. *Id.*
4. *E.g.*, Panavision v. Toeppen, 141 F.3d 1316 (9th Cir. 1998).
5. 15 U.S.C. § 1125(d)(1)(B)(i).
6. *Id.*, § 1125(d)(1)(B)(ii).
7. 52 U.S.P.Q.2d 1402 (D. Mass. 1999).
8. 15 U.S.C. § 1116, § 1117 (a).
9. *Id.*, § 1117(d).
10. *Id.*, § 1125(d)(1)(C).
11. *Id.*, § 1125(d)(2)(A).
12. 51 F. Supp. 2d 707 (E.D.Va. 1999).
13. 15 U.S.C. § 1125(d)(2)(B).
14. *Id.*, § 1125(d)(2)(C).
15. *Id.*, § 1125(d)(2)(D)(i).
16. *Id.*
17. *Id.*, § 1125(d)(3)-(4).
18. *Id.*, § 1114(1)(D)(iv).
19. *Id.*, § 1125(d)1(D).
20. *Id.*, § 1125(d)(2)(D)(ii).
21. *Id.*, § 1114(1)(D).
22. *Id.*, § 1125(d)(2).

▲ ▲ ▲