

Piercing the Registrant's Veil

Trademark Infringement on the Internet, Identifying and Pursuing Infringers, and the Pros and Cons of Proxy Domain Name Registration

by Brett R. Harris, Amanda F. Shechter and Anthony E. Wilkinson

The pursuit of trademark infringers on the Internet, specifically the use of a party's trademark by an unauthorized second party, poses problems that are unique in trademark infringement law. How do you uncover who is the true owner of the website that has made unlawful use of your client's trademark? What tools are at your disposal? What mechanisms, put in place to safeguard the privacy of domain owners, can potentially thwart your discovery?

Identifying the Website Owner

When you find an unauthorized appearance of your client's trademark on a website, you first need to identify the appropriate recipient of a cease and desist letter, the first tool in your anti-infringement toolbox. In certain instances, the infringing website will contain terms and conditions explaining the legal rules for using the site. It may have an intellectual property policy posted, and may even give the name and address of the party to whom you can address the cease and desist letter.

But what if the terms and conditions state the page is actually maintained by someone else, and that the website is not responsible for the content of the page? Or what if there are no terms and conditions, or worse yet, no name, address or other identifying information for the party operating the website? First, you must identify the site's 'owner' in order to bring your complaint to the proper party. Secondly, if need be, you must identify the defendant in the trademark infringement lawsuit you may need to bring, if the owner does not voluntarily stop its infringement of your client's trademark.

It is important to understand what it really means to find a site's owner. A website has a domain name, also known as its web address, which it uses to connect to the Internet.¹ The owner of the website is the person or entity who holds the domain name. The Internet Corporation for Assigned Names and Numbers (ICANN), a private-sector nonprofit corpora-

tion, controls domain name ownership, and not only oversees the coordination of domain names, but also technically ensures that each domain name is associated with the correct computer Internet address.

ICANN makes agreements, called registrar accreditation agreements, with entities called registrars. In order to become the holder of a domain name, one must register the domain name with a registrar. Such a person is called a registrant. The registrant receives a license to use the domain name.

Since the registrant's right to own a domain name comes through its agreement with an ICANN-approved registrar, in order to identify the registrant, one must first identify the registrar.

Consequently, you decide to send a cease and desist letter to the registrar, along with a request for the identity and address of the actual registrant. Unfortunately, the registrar responds by a canned email (with a "do-not-reply" return address) that it does not maintain the website and it does not place content on it. It also states that it is contrary to its policies to reveal the identity of the registrant. Furthermore, the response email notes nothing about whether the unauthorized use of the trademark will stop. A few weeks go by and your client's trademark is still appearing on the infringing website. Now what?

You may decide to review the registrar accreditation agreement (RAA) registrars must execute with ICANN. The most recent version of the RAA, dated May 17, 2001,² can be found

on the ICANN website, www.icann.org.

The RAA requires the registrar to enter into a registration agreement with the registrant (called the registered name holder in the RAA). The RAA states that in such a registration agreement, the registrant must provide the registrar with accurate, reliable and up-to-date contact details.³ Moreover, Section 3.7.8 of the RAA requires the registrar to verify, periodically re-verify, and correct, if necessary, this contact information. However, the RAA does not require the registrar to share this information with the public.

The RAA does require the registration agreement between the registrant and the registrar to include a representation by the registrant that the manner in which the domain name (called the registered name in the RAA) is used will not directly or indirectly infringe the legal rights of any third party. One could argue that the unauthorized use of a third party's intellectual property is precisely such an infringement of these legal rights.

However, ICANN does not provide any means by which your client can force the registrar to require the registrant to abide by the registration agreement. The only dispute procedure ICANN provides is the Uniform Domain Name Dispute Resolution Policy (UDRP) for addressing, through arbitration, a situation in which the domain name itself, rather than the content on the associated website, infringes a trademark. Indeed, in a prepared statement of the Federal Trade Commission before the Congressional Subcommittee on Courts, the Internet, and Intellectual Property, the agency bemoaned the difficulty of getting a registrar to suspend the domain name of a registrant who violates the registration agreement, especially since the registrar receives fees from the registrant.⁴

While this proxy registration has created a roadblock in your attempt to protect your client's intellectual property rights, the fact is that the primary

reason registrars often shield the names of registrants is not for the purpose of aiding trademark infringement, but rather to protect the privacy of the registrant. There are good reasons for this, but the competing interests of privacy for the registrant and disclosure for the aggrieved intellectual property owner must be balanced.

Pros and Cons of Proxy Registration

Pros

As an administrative panel of the World Intellectual Property Organization (WIPO) Arbitration and Mediation Center noted in *HSBC Finance Corporation v. Clear Blue Sky Inc. and Domain Manager*, "Privacy services generally are recognized to perform a legitimate function by shielding registrants from 'spam' as a result of their contact details being made publicly available on the WHOIS database."⁵ The problem of spam is widespread, and both individual and business domain owners have justifiable interest in protecting their domain names from abuse by spammers.

In addition, anonymous registration of domain names is important for the Internet to serve as a forum for public information and free speech, including political, artistic and religious expression. Private individuals (*i.e.*, natural persons rather than businesses) may have a greater privacy interest than commercial websites, since individuals may wish to express their free speech anonymously.⁶

Cons

The benefits of making VeriSign Global Registry Services WHOIS Search data publicly available include protecting consumers from online fraud; facilitating commercial transactions that require due diligence such as mergers and acquisitions, licensing, and secured transaction; and facilitating the management of large domain name portfolios.⁷ Making this data publicly available is also relevant to the prosecution of

intellectual property infringement:

This access enables intellectual property owners to quickly contact the party responsible for the registration or use of a domain name that involves infringement of trademark or copyright, cybersquatting, or other illegal behavior. In most cases, this quick contact leads to a prompt resolution of the problem, without the need to invoke the UDRP or more formal legal processes. In those cases which do proceed to a UDRP complaint, civil litigation, or a criminal investigation, the data currently available in WHOIS is often essential to effective enforcement.⁸

The *HSBC* panel noted that it did not consider the domain name owner's use of a privacy service, in and of itself, to constitute bad faith under the Uniform Domain Name Dispute Policy, but acknowledged that "privacy services are subject to manipulation by a registrant seeking to evade enforcement of legitimate third-party rights or to obstruct proceedings commenced under the Policy or elsewhere."⁹

Further, while privacy or proxy services may protect innocent registrants from spammers, violators of the anti-spam laws can also use the same proxy services to hide their activities by concealing WHOIS data enabling them to use spam, viruses and spyware to infringe third-party rights or otherwise damage third parties.¹⁰

WHOIS databases provide a crucial tool for businesses, the Federal Trade Commission, and other law enforcement agencies to track down brand infringement, online fraud, identity theft, and other online illegal activity, but are often hindered in their pursuit because the person responsible is hiding behind the anonymity of false registration information.¹¹

STEPS TO IDENTIFY THE REGISTRAR AND REGISTRANT

URLs are administered by different accredited registrars. All of the registrars have directories, which tell about registration information on all URLs, but the most comprehensive search is to go to the registry that holds the domain name registration. By way of explanation, the phone book has everyone's telephone listings, but people get their phone service through Verizon, MCI, Sprint, etc. Initially you go to the master directory to see which registrar has the particular registration, then you can go to that registrar's directory to check the domain name registration.

Directions are as follows: First, confirm proper registration of domain name through ICANN at www.internic.net/whois.html, or through VeriSign Global Registry Services WHOIS Search, the database administering .com, .net and .org domain names (at www.verisign-grs.com/whois). Each of these contains a directory known as WHOIS, which allows you to enter a domain name and obtain the name of its registrar. The registrar's contact information, usually including a website, is also provided. Alternatively, for registry contact information, see ICANN's Accredited Registrar Directory at www.internic.net/alpha.html. Then, with this information, you can go to the WHOIS directory on the registrar's website, which contains information about each domain name registered by the registrar, such as the name of the registrant and the administrative contact for communicating with the registrant.

If you follow this procedure to identify the name and address of a registrant, you may be stymied in a variety of ways. First, the registrant may have provided the registrar with an incorrect address. Second, the registrar may have agreed to be the administrative contact for the registrant. In both instances, there is no way for you to send a cease and desist letter directly to the registrant. Third, the registrar may have agreed to shield the identity of the registrant, known as proxy or private registration. In such a case, the name of the registrant will only specify a proxy registrar entity along with some indication that the registrar has agreed to conceal the identity of the registrant. Also, the only contact information will be the address of the registrar entity.

Potential Solutions

ICANN is considering a proposal to create a new contact type called the operational point of contact (OPoC). The OPoC proposal would allow registrants to only publish details of the OPoC. In the case of a dispute involving the domain name, the OPoC would contact the registrant.¹² It remains to be seen, however, whether the OPoC could be named as a defendant in an infringement lawsuit if the OPoC is not the actu-

al owner of the website, or what mechanisms would be in place to ensure a cease and desist letter or complaint forwarded to the OPoC would, in fact, be received by the domain owner. To date, there has been no adoption of the OPoC.

ICANN is in the process of amending the RAA,¹³ however the amendments that were under review by the ICANN board as of March 6, 2009, do not address the concern that registrars do not need to reveal registrant identification informa-

tion, even in the case of trademark infringement. Specifically, a suggestion was made by the Intellectual Property Constituency, an advisory committee of ICANN, that the amended registrar-registrant agreement form, an appendix to the RAA, contain language that makes clear proxies and private registration services must respond to requests for registrant identification information when presented with reasonable evidence of abuse. This has not been addressed in the proposed RAA amendments. ☹

Endnotes

1. For a more complete explanation of the various segments that make up a domain name, see Harris, *Internet Update: Milestone Changes to the Domain Name System Underway*, *New Jersey Lawyer*, December 2008, p.70.
2. Amendments to the RAA have been proposed and were posted by ICANN for public review on Dec. 16, 2008, and approved by the ICANN board on March 6, 2009; however, none of the proposed amendments address the problem of obtaining registrant information. See proposed amendments at www.icann.org/en/topics/raa/redline-2001-raa-25nov08.pdf. A transcript of the motion approving the set of amendments can be found at <http://gnso.icann.org/resolutions/#200903>.
3. *Id.* Section 3.7.7.1 of the RAA.
4. Prepared statement of the Federal Trade Commission on the Integrity and Accuracy of the "WHOIS" Database Before the Subcommittee on Courts, the Internet, and Intellectual Property of the Committee on the Judiciary United States House of Representatives, Washington, D.C., May 22, 2002, page 4, www.ftc.gov/os/2002/05/whois.htm.
5. *HSBC Finance Corporation v. Clear Blue Sky Inc. and Domain Manager*,

- Case No. D2007-0062 (June 4, 2007), footnote 16.
6. Final Task Force Report on WHOIS Services, by GNSO WHOIS Task Force (March 12, 2007), <http://gnso.icann.org/issues/whois-privacy/whois-services-final-tf-report-12mar07.htm>.
 7. Summary of public comments received from September 13 through October 30 on recent GNSO WHOIS Activities, prepared by Liz Gasster of ICANN, Oct. 31, 2007. Public comments are archived at www.icann.org/public_comment/#whois-comments-2007/
 8. Statement of the Intellectual Property Constituency in Final Task Force Report on WHOIS Services, by GNSO WHOIS Task Force (March 12, 2007).
 9. *HSBC Finance Corp.*, at page 14.
 10. Final Task Force Report on WHOIS Services, by GNSO WHOIS Task Force (March 12, 2007), <http://gnso.icann.org/issues/whois-privacy/whois-services-final-tf-report-12mar07.htm>.
 11. 110th Congress, 2nd Session, Senate Bill S. 2661, section 2(15) (introduced Feb. 25, 2008).
 12. Final Task Force Report on WHOIS Services, by GNSO WHOIS Task Force (March 12, 2007), <http://gnso.icann.org/issues/whoisprivacy/whois-services-final-tf-report-12mar07.htm>.
 13. See endnote 2.

firm of Wilentz, Goldman & Spitzer, P.A. or its clients. Website addresses included in this article are provided for reference only, and the authors make no guarantees regarding the accuracy or reliability of the information contained at these websites.

This article was originally published in the June 2009 issue of New Jersey Lawyer Magazine, a publication of the New Jersey Bar Association, and is reprinted here with permission.

Brett R. Harris is a shareholder with Wilentz, Goldman & Spitzer, P.A. in Woodbridge. She is a corporate transactional attorney specializing in advising businesses on technology and intellectual property matters, and counseling Internet and computer companies. **Amanda F. Shechter** is counsel to the firm and **Anthony E. Wilkinson** is an associate of the firm. Both work with Harris on business and intellectual property matters. The views expressed herein are personal to the authors and do not necessarily represent those of the