By **Bruce McDonald**

Why trademark owners must lead the fight for accountability in e-commerce

New proposals on electronic service of process on fictitious and anonymous websites have come under scrutiny, but offer an important tool to fight online fraud

Last year was a banner year for online fraud, with victims reporting over $500 million in losses. The Federal Bureau of Investigation reported 336,655 complaints in 2009 and processed an average of 25,000 complaints per month in 2010. Internet fraud is carried out in large part by fictitious and anonymous persons impersonating, imitating and counterfeiting well-known trademarks and service marks. While not all fictitious and anonymous websites are used for consumer fraud, internet crime is enabled by an astonishing lack of transparency in the registration of domain names, even as the organisation entrusted with internet governance is preparing to roll out hundreds of new generic top level domains (gTLDs).

In response, a proposal has emerged in the trademark community for legislative and treaty amendments that would authorise service of process by electronic mail, without a court order, on the email address for a fictitious or anonymous website in a civil action arising out of the advertising or sale of goods or services at that site. The proposal is currently the subject of debate at the International Trademark Association (INTA) and the American Bar Association (ABA).

The scope of the problem

A number of issues exist with regard to online fraud. In terms of consumer fraud, a common example involves the use of a well-known company name being counterfeited by scammers to swindle consumers. A website appears under using the name of a company – for instance, the fictitious 'Famous bank' could be used to create 'famousbankfinance.com'. After entering his personal information into a dialogue box, a consumer receives a call from 'Famous bank' informing him that loan approval has been granted, but that because of his credit score, the loan must be secured by a security deposit in the amount of $1,250. The consumer then receives an email appending an application, which is signed and faxed back to a toll-free number with the number of his bank account. He then receives another call with wire instructions and ultimately sends the advance payment, joining half a million others who will be victimised this year in a similar manner.

Half a million may sound like a large number of fictitious and anonymous commercial websites, but the real number is exponentially larger due to the extraordinary volume of counterfeit domain names used for pay-per-click advertising websites.

The revenue stream for pay-per-click advertising begins with an advertiser which purchases from a search engine a trademark or service mark that it does not own (eg, 'Citibank') for use as a keyword. The advertiser pays the search engine for every hit that the search engine sends to the advertiser's website.

However, counterfeit websites are often set up by fictitious and anonymous third parties to attract internet traffic, drawing in consumers who attempt to type, say, 'Citibank' into their website browsers but type the misspelled name 'Citiebank' instead. The counterfeit website, by means of links that display the correct name Citibank, then redirects consumers to the website of the advertiser and the search engine operator pays the counterfeit website owner for every hit that is redirected to the advertiser's website. The revenues earned in this manner amount to several billion dollars annually.

The legality of pay-per-click advertising based on the unauthorised sale of trademarks for use as keywords is a controversial issue. However, the use of trademarks as keywords is to be distinguished from the surreptitious registration of domain names to fictitious entities and anonymous persons, which, if undertaken for keyword advertising or other commercial purpose, results by definition in concealment of the origin and source of goods and services advertised and sold on the Internet.

Institutionalised concealment

While many domain names used for pay-per-click advertising are generic, the vast majority infringe trademarks by typo-squatting (eg, citiebank.com) or combo-squatting (eg, famousbankloans.com or famousbankcredit.com). By 2008, the registration of such domain names exceeded 350,000 per month. Ownership of such names is viable only if concealed; otherwise, it would entail massive liability for trademark infringement.

Theoretically, it should be possible to identify the person legally accountable for a commercial website. In 1998 responsibility for this elementary component of internet governance was entrusted by Congress to the Internet Corporation for Assigned Names and Numbers (ICANN). Pursuant to a contract with the US Department of Commerce, ICANN is required to provide for a publicly accessible, searchable database of contact data for the owners of domain names in gTLDs – the repository of information known as the WHOIS database.

To engage in domain name registration services, registrars are required to enter into registration accreditation agreements with ICANN that obligate them to ensure accurate and current contact data in the WHOIS database for internet domain names registered by them. ICANN, however, has been unable to enforce this requirement and has further allowed the concealment of ownership data through "proxy" or "privacy" services, which are unabashedly advertised as a means of evading the WHOIS requirement. ICANN's failure to enforce the WHOIS requirement, depending on whose opinion is consulted, has either caused or resulted from an exponential growth of domain names registered to fictitious entities, sham companies and unidentified individuals ostensibly located at non-existent addresses.

The absence of transparency and accountability in domain name ownership is complicated – perhaps fatally – by ICANN's financial dependence on the stimulation of new domain name registration

and registrar accreditation. Internet domain name registrars are accredited by ICANN to purchase domain names directly from registries and sell them to the public. Each gTLD has a single registry, but there is no limit to the number of registrars that may be accredited by ICANN. In 1999 there was one ICANN-accredited registrar; by 2003 there were approximately 60; today there are 1,000 or more. ICANN touts this exponential growth in the number of accredited registrars as a sign of its success.

However, ICANN also has an inherent interest in the stimulation of new domain name registration. Each newly minted registrar pays an application fee to ICANN in the amount of $2,500, an annual accreditation fee of $4,000 and a variable annual fee of between $1,200 and $2,000, as well as a transaction fee of $0.20 for every new domain name registration. The financial incentive for ICANN to promote the maximum growth of new internet domain name registrations and accreditation of registrars is profoundly peculiar and, by encouraging the surreptitious registration of domain names, undermines the rule of law.

The ease and impunity with which registrants conceal their identity is fuelling controversy over the adequacy of ICANN's performance, driven by a conflict between two polarised camps. On one side are consumers, rights holders, law enforcement agencies and other groups interested in public access to information about the ownership of commercial websites. The other side is represented principally by internet domain name registrars, which argue that the disclosure of such information violates the privacy and First Amendment rights of their customers.

Undoubtedly, there are persons and organisations with a legitimate interest in the privacy of information about ownership of non-commercial websites. However, should privacy extend to the ownership of *commercial* websites? And why have so many domain name registrars taken up the banner of privacy in the absence of evidence that their class of customers includes any organisations with *bona fide* privacy concerns?

The trademark community responds

If approved, a proposal from INTA's Internet Committee would result in INTA's advocacy of legislative and treaty amendments. It provides that "in a civil action arising out of the advertising or sale of goods and services via a fictitiously owned commercial website, service of process by electronic mail on the e-mail address provided in the WHOIS record associated with the domain name for that website shall be effective against the named registrant without the need for a court order allowing for substituted service".

In June 2010 the ABA Section of Intellectual Property Law provided comments in which it agreed that the creation of a mechanism for substituted service of process – one which would not require prolonged efforts to discover the actual physical location of the real website owner and to serve process at such physical location – would be highly beneficial to the public, rights holders and other aggrieved parties, and would ensure that courts can adjudicate claims arising out of these unlawful actions. However, the ABA also raised certain issues, including concerns about due process and freedom of speech, as well as a request for clarification regarding the relationship between the registrant and others associated with a domain name. In response, an amendment to the proposal is under consideration to the effect that a website shall be deemed to be "fictitiously" or "anonymously" owned only when concealment of ownership is a "direct result and necessary consequence of false or incomplete WHOIS information."

Anonymous commerce and due process

There is no tradition of anonymous commerce in the United States. The laws in all 50 states require vendors to designate themselves or an agent for service of process in actions arising out of the advertising or sale of their goods and services. The surreptitious conduct of business via mail, wire, radio or television using a fictitious name to conceal one's identity is an indictable offence. In Europe, it is no different; Article 5 of the E-commerce Directive provides that all service providers shall "render easily, directly and permanently accessible to the recipients of the service and competent authorities… the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner".

On due process, US courts have held that while a plaintiff is entitled to bring suit against an anonymous defendant, the plaintiff must sufficiently identify the defendant to enable service of process that will allow the court action to proceed. However, the law has "long recognised that, in the case of persons missing or unknown, employment of an indirect and even a probably futile means of notification is all that the situation permits and creates no… constitutional bar to a final decree foreclosing their rights" (*Mullane v Central Hanover Bank & Trust Co*, (339 US 306, 317 (1950))). Thus, US courts allow electronic service of process where a defendant has attempted to evade service and is reasonably accessible only by electronic mail.

To obtain authorisation for electronic service, however, parties may be required to engage in efforts to effect service by traditional means that are futile, expensive and time consuming, and must then incur the additional time and expense of obtaining a court order allowing for substituted service.

Advocates of the electronic service proposal believe that due process will be satisfied without such efforts if a website and domain name are deemed fictitiously owned only when concealment of the true ownership is a direct result and necessary consequence of the false or incomplete WHOIS information, and that a reasonable definition of 'fictitious' and 'anonymous' will adequately ensure that objective facts and circumstances are not disregarded in this determination. If the ownership of a website or domain name can be reasonably ascertained from factors outside the four corners of the WHOIS database and the content of the website, there is no basis to allow service of process by electronic mail with or without a court order.

Attempted communications

An important question is whether the plaintiff must first attempt to communicate with the fictitious registrant prior to effecting service. The purpose of such communication is to establish that the registrant responds to such communications and, to that extent, is likely to receive actual notice. The problem with this requirement is that this validates a cat-and-mouse game in which the registrant is rewarded for ignoring communications from the public.

Where a domain name and website are used for the advertising and sale of goods and services, and there is no other means by which the public can reasonably identify the origin and source of such goods and services, the law should require the registrant to be aware of what is sent to the email address listed in the WHOIS database. The registration of that email address should be construed as consent to service of process in an action arising out of goods and services advertised or sold at that website – the definition of 'fictitious' and 'anonymous' can be tailored to ensure that electronic service without a court order is authorised only in instances where no other method of service is reasonably available.

The elimination of a hearing on a motion for substituted service of process will not deprive the fictitious and anonymous domain

name registrant of due process in the limited circumstances contemplated by the INTA Internet Committee proposal, as the defendant will also be entitled to notification prior to entry of default judgment and again prior to the proof of damage hearing. Moreover, if the defendant elects to remain anonymous instead of identifying himself in such proceedings, then the court cannot issue a judgment against him except in his capacity as a 'John Doe'. Prior to the enforcement of an award against this John Doe in the form of a subsequent attachment or collection action, the plaintiff will again have to prove that this person is the same John Doe named in the judgment, at which time the defendant will have yet another opportunity for an evidentiary hearing.

Turning to international comity, US courts are holding with increasing frequency that electronic service on fictitious and anonymous commercial websites comports with international standards. Conceptually, electronic service complies with Article 5 of the Hague Convention, which provides that documents "may always be served by delivery to an address who accepts it voluntarily". Viewing the EU E-commerce Directive as a relevant statement of principle, it is reasonable to advocate an amendment to the Hague Convention providing that in an action arising out of the sale or advertising of goods or services at a fictitious or anonymous website, registration of the email address associated with the domain name used for that website "shall constitute the voluntary acceptance of document sent to that email address".

First Amendment considerations

The most controversial issue raised by the INTA Internet Committee proposal is the scope of First Amendment protection for commercial speech on the Internet, and whether that protection extends to the concealment of the origin and source of goods and services. Opponents of the electronic service proposal argue that, even if electronic service is limited to actions involving commercial websites, it nevertheless has the potential to implicate First Amendment concerns by impinging on the right to speak anonymously, as in a commercial website run by an author operating under a pseudonym for the purpose of advertising and selling his pseudonymous publications.

Clearly, the First Amendment includes the right to speak anonymously. Moreover, the First Amendment places anonymous speech on the Internet on the same footing as other speech. As with other forms of expression, the ability to speak anonymously on the Internet promotes the robust exchange of ideas and allows individuals to express themselves freely without fear of economic or official retaliation or concern about social ostracism. The importance of the Internet to the expression of protected speech cannot be overstated.

The right to political expression, however, does not extend to commercial speech. Laws which restrict core political speech are subject to exacting scrutiny – even if they leave citizens with other means to disseminate their ideas. Commercial speech, on the other hand (ie, "speech which does no more than propose a commercial transaction") is not entitled to the same protection (*Posadas de Puerto Rico Associates v Tourism Co of Puerto Rico*, 478 US 328, 339 (1986)).

There is no authority for the proposition that persons may exploit their anonymity on the Internet to evade accountability that would attach in any brick-and-mortar environment relating to the origin and source of goods and services. Nor does the First Amendment provide a licence for IP infringement.

In *American Civil Liberties Union v Miller* (977 F Supp 2d 1228 (NDGa 1997)), internet users challenged the constitutionality of a state criminal statute prohibiting internet transmissions which falsely identified the sender or which used trade names or logos which would falsely state or imply that the sender was legally authorised to use them. The court granted the plaintiffs' motion for a preliminary injunction, holding that they were likely to succeed on their claim that the statute imposed content-based restrictions which were not narrowly tailored to achieve a compelling state interest, and that the statute was unconstitutionally overbroad and vague.

The *Miller* decision, however, was rendered before the courts or the public could predict how the commercial electronic landscape would appear some 14 years later, and has been distinguished in cases that are more relevant to current realities, such as *Gucci America Inc v Hall & Associates* (135 F Supp 2d 409, 418 (SDNY 2001)). In this case the owner of a trademark brought an infringement action against a website operator and the internet service provider (ISP) that was hosting the operator's site.

The district court denied the ISP's motion to dismiss, holding that the First Amendment did not bar a claim that the ISP's hosting of an infringing website was itself an infringement of the owner's mark inasmuch as deceptive commercial speech is not protected by the First Amendment (see also *Arista Records LLC v Doe 3*, 604 F 3d 110 (2d Cir 2010)).

In summary, the online pseudonymous bookseller must be equated to any other bookstore selling copies of pseudonymous publications and held to the same standard as any other commercial establishment in relation to his own identity. If he wants to protect his identity, he can form a corporation like any other individual and designate an agent for service of process. The right to publish pseudonymously does not entitle him to operate a clandestine bookselling business.

Ultimately, the lack of transparency and accountability in the registration of internet domain names used for commercial websites is a major factor in internet fraud, including trademark and service mark counterfeiting in which consumers and trademark owners are equally targeted. While not all internet fraud involves counterfeiting, trademark and service mark owners are uniquely affected by the extraordinary volume of domain names registered to fictitious and anonymous entities. Where a fictitious or anonymous owner of a commercial website has concealed its identity in violation of applicable business and fictitious name requirements, and such concealment is a direct result and necessary consequence of false or incomplete WHOIS information, a growing number of practitioners in and outside of the trademark community believe that service of process by electronic mail at the corresponding WHOIS address should be available, without a court order, in actions arising out of the advertising and sale of goods and services at that website.

Ultimately, with consumers lacking the means to facilitate effective change and law enforcement authorities overwhelmed with other priorities, it is crucial that trademark owners lead the fight for transparency – even though it is a struggle that they did not seek. WTR

Bruce McDonald is a shareholder in the trademark practice group at the law firm of Buchanan Ingersoll & Rooney
bruce.mcdonald@bipc.com