EVICTING THE SQUATTERS

The expansion of available domain names continues apace. New gTLDs and more opportunities to use ccTLDs provide businesses with extra places to do business online. But with that comes danger, as Claudia Strola explains.

All companies and business people have an obvious interest in registering domain names corresponding to their most famous trademarks, the names of their products or their business names.

This growing need has meant that since the launch of the Internet, new and previously unknown types of illegal activity known as cybersquatting and typosquatting have evolved around domain name registration.

The expression cybersquatting (or other similar terms such as domain-grabbing or domain-squatting) is used to describe the practice of buying up domain names corresponding to the proprietary titles of others (trademarks, signs, company names, proper names of famous people, etc.) by unauthorised parties for speculative purposes.

This is done in order to make a profit from:

- Transfer of the domain from the unauthorised owner to the rightful owner, sometimes for very considerable sums
- Use of the domain as a platform for e-commerce for the sale of inauthentic products to thousands of users who are often unaware that the website is not authentic.

In the years following the launch of the Internet and the organisation of a system for registering domain names, the phenomenon exploded, giving rise to rather unfortunate instances of speculation.

Cases in point would be the sale of very attractive domain names, such as mcdonalds.com, to their rightful owners, sometimes at huge prices.

This type of cybersquatting was able to spread thanks to the basic principle governing assignment of domain names: the 'first come, first served' rule. The registration authorities allowed themselves to be guided by a purely chronological criterion: the first applicant for registration of a domain name was assigned that domain name.

The United States was the first country in the world that felt the need to take stern countermeasures against this trade and to adopt specific legislation in the form of the Anticybersquatting Consumer Protection Act, which came into force on November 29, 1999.

Italy does not have specific legislation in this area, and so existing jurisprudence has tended to use applicable regulations in the area of trademarks and distinctive signs. The owner of a registered trademark has the right to its exclusive use and therefore also to register it as a domain name.

Should anyone register and use the trademark of another as a domain name, the owner is entitled to take fast-track legal action, challenging wrongful registrations even of domains with supranational extensions, such as .com, or the national extensions for any given country.

It should be noted that the trademark in question need not even have been registered with the relevant trademarks and patents office. The important thing is that it is sufficiently well known to allow its owner to claim a so-called '*de facto* trademark' right.

Nowadays, domain grabbing is focused on domain names with the extensions of emerging economies, such as China and India, thus underlining that the phenomenon continues to grow. And it would not seem unreasonable to foresee further developments because of the recent admission of top-level domain names with more than 100,000 non-Latin characters.

Typosquatting, also called 'URL hijacking', is the expression used to describe a concept similar to cybersquatting, based on typing errors or 'typos' committed by Internet users when inputting web addresses (or URLs) into software for accessing web information resources (browsers).

Users making these typos often find themselves shunted onto an alternative site registered to a cybersquatter. The phenomenon is huge, with millions of typosquatted domains now in existence.

The typosquatter's URL is very similar to that of the original domain, but it is not identical to the registered trademark. Let us take some examples for the hypothetical domain 'trademark.com':

1. tredemark.com—a common misspelling, or foreign language spelling, of the intended site

2. tradmark.com or trademar.com—a simple misspelling based on typing errors
3. traedmakr.com—an inversion of two or more characters
4. trademarks.com—a differently phrased domain name.
5. trademark.org—the domain main given a different suffix.

Once on the squatter's site, the user can be easily misled into thinking that this is in fact the original domain. Indeed such sites often use similar logos or similar structure/appearance/content to the original site. The user might be unlikely to realise that they have stumbled onto a false site.

This non-original site might very easily become an e-commerce platform and thus generate profits for the squatter by sale of products to users unaware of the inauthenticity of the web page.

Additionally, the typosquatter might use advertising banners on its domain, bringing in yet further revenue.

Here again, the rights holder or owner of the original domain often buys out the false domain in an exercise in damage limitation.

And so, in a scenario that is in constant and rapid evolution, how can legitimate rights holders defend themselves against such ever-present threats, and the consequent loss of earnings and damage to their image?

A number of options are available.

First of all, an efficient control/monitoring strategy is required for tracing false domains among the millions of domains already existing and that continue to be registered across the world.

Secondly, information must be obtained on the owners (for example, name, main office, address, telephone, email, etc.), which is often no easy feat. This data is often kept from public view by using 'privacy shields' offered by some providers in order to protect the identities of owners of domain names.

This renders necessary searches and/or monitoring (surveillance) among national and supranational domain names registered across the world that are similar or identical to a given sign (be it a trademark, a company name, a brand or a proper name), using special software or analysis tools. This is one way of tracing cybersquatted domains.

Such monitoring and surveillance activity may even be applied to typosquatting. This involves tracing a great variety of possible combinations of typos when monitoring a sign: for example, a search for the 'abc' trademark will allow tracing of 'acb', 'cba', 'abcs', etc.

Thus a constantly updated picture may be obtained of the registrations that might potentially interfere with a given trademark of interest.

> "ONCE WRONGFULLY REGISTERED DOMAINS HAVE BEEN TRACED AND THE RELEVANT INFORMATION HAS BEEN OBTAINED ON THEIR OWNERS, IT IS TIME TO TAKE APPROPRIATE ACTION TO PROTECT PROPRIETARY RIGHTS."

Once wrongfully registered domains have been traced and the relevant information has been obtained on their owners, it is time to take appropriate action to protect proprietary rights. The type of action deemed appropriate might vary depending on a number of factors, such as, to cite just a few, the state within which a domain is registered, the counterparty in question, the number of domains registered to that party and the use made of such domains.

Specific channels of action are available:

- Administrative reassignment procedures made available by the national and supranational registration authorities
- A more purely juridical approach, with the sending of cease and desist letters, and action taken before the ordinary courts.

Administrative reassignment procedures are in fact forms of alternative dispute resolution (ADR). As the name implies, these are alternatives to recourse to ordinary courts and are based on simplified premises that exist alongside the principles governing applicable legal regulations in the area of distinctive signs.

They also offer the advantage of being swifter, simpler and less costly than the courts.

ADRs include the type adopted by the World Intellectual Property Organization (WIPO), the oldest and the most tried and tested such alternative procedure in this area. At first, it was applied only to domain names registered with generic extensions (so-called gTLDs). Nowadays, it may also be used with other generic extensions introduced over the years (such as .biz, .info, .aero, .asia, .cat, .coop, .jobs, etc.) and with many domain names registered with national suffixes (so-called ccTLDs).

Based on the WIPO model, several national registration authorities (including the Italian authority) have adopted similar procedures, which like that used by WIPO, have the advantage of being swifter, simpler and less costly.

It should be noted that the procedure can only result in assignment of the domain name to its rightful owner or cancellation.

There is, however, always the option of bringing a purely legal action. Prior to taking an administrative or ordinary court action, it is advisable to send a cease and desist letter, in order to see whether the matter may be settled amicably. If this is not possible, court actions may be taken. But these take much longer and involve considerably higher costs. ■

Claudia Strola is head of MCR Ricerche, a part of the Rapisardi Intellectual Property Group. She can be contacted at: rapisardi@rapisardi.com

Claudia Strola is head of MCR Ricerche, the firm within the Rapisardi intellectual property group that specialises in IP searches, surveillance and investigation. She holds a degree in politics with a major in social research methods from the University of Milan. She has acquired extensive experience in research and surveillance for all industrial property purposes, in accessing data rooms and in drawing up due diligence reports.