# Defeating trade mark infringement on the internet and beating the cybersquatters

*Anna Carboni & Jane Cornwell, Linklaters & Alliance**

Anna Carboni has been a partner in Linklaters' Intellectual Property, Technology & Communications Department since 1996 and is currently on the International Partnership Committee of the firm. Anna advises on a wide range of contentious and non-contentious matters involving intellectual property, information technology and trade secrets. Jane Cornwell has a degree in Law from Cambridge University and trained as a solicitor at Linklaters. She has been an associate in the Intellectual Property & Technology Department since March 2001 and works principally in trade mark filing and prosecution.

## A. Introduction

The purpose of this paper is to look at cybersquatting and on-line trade mark infringement from a legal and practical perspective.[1] Concentrating on litigation in the English courts, it considers a number of important issues such as:

(i) obtaining jurisdiction over the defendant;
(ii) the relevant causes of action and any important limitations likely to cause problems in the Internet context;
(iii) tactics, including the availability of interim relief and summary judgment;
(iv) available remedies; and
(v) any particular risks run by starting cybersquatting or trade mark infringement litigation.

This paper then goes on to consider similar issues arising under US law and under the ICANN and Nominet UK dispute resolution procedures. It finishes with a discussion of recent developments in cybersquatting, on-line trade mark infringement and a comparison of how these developments have been tackled under English law, US law and the ICANN dispute resolution procedure.

## B. Litigation in the English Courts

This section highlights the most important aspects of English intellectual property litigation likely to arise in an Internet infringement context. In particular, it looks at:

(i) the basis upon which a brand owner can bring proceedings in the English courts against a foreign defendant;
(ii) the causes of action available under English law and any pitfalls likely to arise in their application in an Internet context;
(iii) tactics (such as obtaining interim relief and applying for summary judgment);
(iv) remedies; and
(v) the particular risks which a brand owner runs in commencing proceedings in the UK.

### 1. Overcoming the jurisdictional hurdles - foreign defendants

Before starting proceedings, a brand owner should always try to identify as precisely as possible the person or entity which has committed the acts about which it wishes to complain. This will not necessarily be as easy as it sounds: for example, while it should be possible to identify a domain name registrant by consulting the relevant registry database or a website such as www.allwhois.com, it is quite possible that a cybersquatter or on-line infringer may have given incomplete or incorrect details to the domain name registrar in order to evade litigation. In such a case, identifying and tracking down the correct defendant can involve calling on the assistance of private investigators or persuading the court that e-mail can be used to start off proceedings.

Assuming that it is possible to identify and locate the cybersquatter or on-line infringer, the position is broadly as follows:

#### 1.1 Defendant located within the EU/EFTA

Whether the defendant may be sued in the English courts is determined in accordance with the Brussels Convention 1968.[2] The English court's permission is not needed to start proceedings against a foreign defendant if the Brussels Convention applies.[3] Essentially, a brand owner will be able to sue in England on one of two bases, namely:

(i) if the defendant is domiciled in England or Wales; or alternatively
(ii) if the infringing acts have been carried out and/or damage has occurred in England or Wales (this will generally always be the case where the intellectual property rights relied upon are UK trade mark registrations/applications or a right in passing off).[4]

In any event, where the case gives rise to issues as to the validity of the brand owner's rights (such as in a counter-claim for invalidity) the English courts will generally have exclusive jurisdiction over the case and it will not be possible for it to be heard elsewhere.[5]

A brand owner should, in all cases, try to establish whether the defendant is an individual or a corporate entity, as this may affect the place of domicile of the defendant.

#### 1.2 Defendant located outside the EU/EFTA

If the defendant is located outside the EU/EFTA, the Brussels Convention will not apply. The brand owner will have to seek the English court's permission to start proceedings against that defendant. This

permission is discretionary and will depend upon the claimant proving:

(i) that he believes that his claim has "reasonable prospects of success";
(ii) the defendant's address or, if not known, the place or country in which the defendant is likely to be found; and
(iii) that the claim falls within the list of permissible grounds for service outside the jurisdiction set out in Rule 6.20 of the Civil Procedure Rules.[6]

The grounds set out in rule 6.20 which may be of use in an on-line infringement case may include: Rule 6.20(2) (the claimant is seeking an injunction to stop the defendant doing something within England and/or Wales); Rule 6.20(8) (the claim relates to a tort committed or causing damage in England and/or Wales); and Rule 6.20(10) (the claim relates to property situated in England and/or Wales).

## 2. Causes of action

English law deals with cybersquatters and other Internet trade mark infringers by recourse to registered trade mark infringement and the common law doctrine of passing off, as extended by the concept of the "instrument of fraud".[7]

### 2.1 Passing off

The decision of the Court of Appeal in *One In A Million* is the leading authority on cybersquatting under English law.[8] It has been widely quoted and applied and evinces an unequivocal attitude towards cybersquatters:

> *"Any person who deliberately registers a domain name on account of its similarity to the name, brand name or trade mark of an unconnected commercial organisation must expect to find himself on the receiving end of an injunction to restrain the threat of passing off, and the injunction will be in terms which make the name commercially useless to the dealer."*[9]

#### 2.1.1 Basic requirements for passing off

Lord Diplock specified five requirements for the tort of passing off in the decision in *Erven Warnink v. Townend.*[10] There must be:

(i) a misrepresentation;
(ii) made by a trader in the course of trade;
(iii) to prospective customers of his or ultimate consumers of goods or services supplied by him;
(iv) which is calculated to injure the business or goodwill of another trader (in the sense that this is a reasonably foreseeable consequence); and
(v) which causes actual damage to the business or goodwill of the trader by whom the action is brought or (in a quia timet action)[11] will probably do so.

#### 2.1.2 One In A Million

Lord Diplock's five requirements transpose relatively easily into an Internet context where the defendant is actually trading from his website. This can be broadly assimilated to a traditional passing off scenario in which the defendant misrepresents that his goods, services or shop are those of the claimant or are in some way linked to the claimant's business.

The first and last elements of Lord Diplock's formulation were, however, extremely problematic in straight cybersquatting cases. It is difficult to infer from the simple act of registration any form of representation to consumers; without use of the domain name, or a threat to use it or to sell it to a third party, it is equally difficult for the claimant to point to any damage, whether actual or threatened. Given this, it was generally thought necessary to wait for an express threat by the cybersquatter that he intended to sell or use the disputed domain name before an action in passing off could be brought. So-called "blocking registrations" could not be pursued.

In *One In A Million* the Court of Appeal moved away from this position. It extended the hitherto accepted rules of passing off in order to catch "blocking registrations" by developing the concept of the "instrument of fraud". The Court of Appeal ruled that the mere adoption of a trading name (whether on the Internet, in the form of a domain name registration or otherwise) can give rise to a misrepresentation that the trader is, in fact, another trader or is in some way connected to that other trader.

The main effect of the decision is that, in the case of household names, it is no longer necessary to wait for an express threat by a cybersquatter that he intends to sell or use a disputed domain name. The owner of the household name can take action against a cybersquatter as soon as it is known that the registration has taken place. "Going equipped" with or creating an instrument of fraud is no longer only actionable in a *quia timet* action for threats to commit passing off. It is a basis for attack in its own right.

In summary, the Court of Appeal summarised the three scenarios in which it could grant an injunction for passing off as follows:[12]

> *"It follows that the court will intervene by way of injunction in passing-off cases in three types of case. First, where there is passing off established or it is threatened. Secondly, where the defendant is a joint tortfeasor with another in passing off either actual or threatened. Thirdly, where the defendant has equipped himself with or intends to equip another with an instrument of fraud."*

#### 2.1.3 Distinctive and non-distinctive brand names

A claimant must have some "badge of recognition" upon which to found his claim to goodwill. In the Internet context, this will generally involve either a trade mark (registered or otherwise) or some other trading or personal name.

The Court of Appeal made it clear in *One In A Million* that whether the circumstances are appropriate for the grant of an injunction (which is, after all, a discretionary remedy) would depend largely upon the nature and distinctiveness of the domain name registered. The key question is

whether the disputed domain name registration is "inherently deceptive". If it is, then the domain name registration will automatically be an instrument of fraud (and damage is presumed). If it is not inherently deceptive, the registration may still amount to an instrument of fraud, but this must be proved on the facts in each case.[13]

It will obviously be easier to show that a domain name registration is an instrument of fraud if the name is one in which no third party could have a legitimate interest co-existent with the interest of the claimant. This is evident from the case law which has followed *One In A Million.*[14]

#### 2.1.4 Recent cases on descriptive and generic brand names

The need to show that an impugned domain name registration is deceptive will cause particular problems for businesses which have developed brand names which are arguably descriptive and/or generic. This has previously given rise to litigation in the English courts. The traditional test as to whether a mark is merely generic or descriptive is to be found in 19th century English case law. Essentially, an English court will ask whether the brand name merely forms part of "the common stock of language" or has come to have a particular meaning relating to the brand owner.[15]

The English cases applying this test to domain name registrations do not give a particularly clear indication of the court's likely approach in any given case. However, it is clear that being able to demonstrate goodwill in the chosen brand name and/or consumer confusion assumes considerable importance where potentially descriptive or generic names are concerned.

On the one hand, the English courts seem unwilling to provide protection in passing off to brand names which are based on "e-language" words. In the recent *eFax.com* decision,[16] the judge noted:

> *"... to anyone remotely familiar with the internet and with e-mail the prefix "e" is shorthand for electronic and refers to the internet. What might be described as an "e-language" is rapidly growing, a language which, as I see it, is likely to render Lord Hershall's concept of "the common stock of the language" more and more difficult to apply".*

The judge concluded that, although not bound to fail at trial, the claimant would have "a difficult task" in proving passing off based on the brand name "eFax". He considered that confusion caused by the parties offering competing services under the "eFax" name would be due to the descriptive and generic nature of the word, rather than to any representation by the defendant. He also noted that there were significant differences between the parties' respective businesses which would alert any visitor to the defendant's website that it was not that of, or to linked to, the claimant. The judge declined to grant injunctive relief in favour of the claimant.

On the other hand, where the brand owner is able to adduce evidence of goodwill attaching to his name or evidence of consumer confusion, he/she may have better prospects of success. In the more recent *lawyeronline.co.uk* case, the judge held that the claimant's domain name *lawyersonline.co.uk* was capable of protection under the doctrine of passing off.[17] This was notwithstanding the fact that it was descriptive of the services provided through the claimant's website.

The judge rejected the proposition that there could never be a proprietary interest in a generic or descriptive word. Instead, on the basis of the claimant's use of the domain name and substantial advertising campaign, the judge concluded that there was at least *prima facie* evidence that goodwill had attached to the claimant's domain name and that some consumers had been confused by the defendant's operation of a similar service under the name *lawyeronline.co.uk.* The judge granted an interim injunction in the claimant's favour.

### 2.2 Registered trade mark infringement

Developments affecting English law post-*One In A Million* have not been confined to the doctrine of passing off.[18] However, while their approach to passing off has been flexible and expansive, the English courts have shown themselves to be unwilling to manipulate the boundaries of registered trade mark infringement to quite the same degree.

#### 2.2.1 Basic requirements for a registered trade mark infringement claim

Infringement of a UK registered trade mark is governed by section 10 *Trade Marks Act 1994.* Infringement will take place upon:

(i) use of an identical mark in relation to identical goods/services (section 10(1));

(ii) use of an identical or similar mark in relation to identical or similar goods/services in circumstances in which the public is likely to be confused (section 10(2)); or

(iii) use of an identical or similar mark in relation to dissimilar goods/services where the claimant's mark has a reputation in the UK and the defendant's use of the mark takes unfair advantage of or is detrimental to the distinctive character or the repute of the mark (section 10(3)).

None of these things will amount to an infringement if the exceptions set out in sections 10 and 11 of the 1994 Act apply. For example, there will be no infringement where the defendant is acting in accordance with honest commercial practices and using the mark to identify the goods as those of the proprietor or to indicate the nature and purpose of the goods. As a result, it may be difficult to pursue for trade mark infringement any third parties who trade in a brand owner's goods on-line, but who correctly identify the brand owner as the source of those products.

#### 2.2.2 The need to show use of the infringed mark within the UK

For there to be infringement under the 1994 Act, there must be use of a trade mark in the course of trade in

the UK.[19] This requirement can cause considerable difficulties where a website containing a brand owner's marks is being operated from outside the UK.

In two recent appeals from the UK Trade Marks Registry, Jacob J has made it clear that it is not sufficient for this purpose that the disputed website is accessible from the UK.[20] Rather, there must be some evidence that the website in question is directed towards the UK for a claim under the 1994 Act to be made out.

In both cases, it was argued by the brand owner that a website is "omnipresent" in cyberspace. Placing a trade mark on a website is, therefore, the equivalent to "putting a tentacle" into the premises of all computer users in all jurisdictions, including the UK. This argument was roundly rejected by Jacob J. He said:

> *"For trade mark laws to intrude where a website owner is not intending to address the world but only a local clientele and where anyone seeing the site would so understand him would be absurd... the mere fact that websites can be accessed from anywhere in the world does not mean, for trade mark purposes, that the law should regard them as being used anywhere in the world. It all depends upon the circumstances, particularly the intention of the website owner and what the reader will understand if he accesses the site".*

Jacob J's decisions have generally been welcomed by English commentators. He was clearly keen to avoid a situation in which the display of an English registered mark on a website run from anywhere in the world could amount to infringement of that trade mark registration.

Looking at the issue more broadly, however, the decisions are not without their difficulties for brand owners, particularly those who take the pre-emptive step of registering a trade mark "defensively" in the UK with a view to thereby protecting their rights in the second level domain name in the UK. It is the logical consequence of Jacob J's decisions that use of the trade mark on a website run from outside the UK may not amount to "use" for the non-use revocation provisions of the 1994 Act.[21]

However, both decisions do leave some latitude for brand owners to argue that they do have sufficient goodwill or have marketed their trade mark sufficiently in the UK for use on a website run from outside the UK to amount to "genuine use" of the mark within the UK. Jacob J cited as an example of this *amazon.com*, a company which had "actively gone out to seek world-wide trade" and which operated a "real supply service" into the UK.

### 3. Tactics and interim relief

Court proceedings are often regarded as being drawn-out and expensive. However, putative claimants should not forget the possibility of applying for interim relief, typically taking the form of an interim injunction, and/or summary judgment against the defendant.

#### 3.1 Interim injunctions

As in any intellectual property litigation, one of the most common orders sought in cybersquatting and on-line infringement cases is an injunction requiring a domain name registrant not to use a domain name registration pending full trial of the dispute. In practice, interim injunctions of this kind are very important and may dispose of the action altogether. In certain circumstances, it may be possible to apply for these injunctions without having to give notice of the application to the defendant.

The basic principles by which an English court will decide to grant an interim injunction are set out in the decision in *American Cyanamid -v- Ethicon*.[22] The court will consider:

(i) whether there is a serious question to be tried (if no, no injunction);

(ii) whether damages would be an adequate remedy for the claimant at trial and whether the defendant would be able to pay them (if yes, no injunction);

(iii) whether effects of the injunction on the defendant could be adequately compensated by an undertaking in damages by the claimant (if no, no injunction);

(iv) in whose favour the balance of convenience (i.e. the balance of the risk of doing one of the parties an injustice) lies.

In circumstances where the grant of the interim injunction is likely to dispose of the case completely, the court may also look at the merits of the parties' cases. The court may also consider any special circumstances and any delay by the claimant in applying for the interim injunction. If the claimant is successful, he will always be required to give an undertaking in damages to protect the defendant in the event of the claim proving unfounded at trial.

Brand owners should note that, where there is likely to be a genuine dispute as to entitlement to use a name (for example, where the defendant may have a legitimate interest in the brand name for some reason), the courts may be hesitant to grant interim relief which effectively requires the defendant to stop trading.

For example, in *MBNA America Bank NA -v- Freeman*, MBNA failed to obtain interim relief suspending use of the domain name *mbna.co.uk* pending trial.[23] MBNA held domain name registrations for *mbna.com* (from which it conducted its Internet business) and *mbna.shopping.com* and *mbna.offers.com* (from which it intended to operate financial and credit card services). The Bank was also owner of a Community trade mark registration for "MBNA". The defendant had not set up an active website under the domain name at the time of the hearing, but claimed that he intended to use it for a business called "Marketing Banners for Net Advertising".

MBNA sought interim injunctions (i) restraining the defendant from operating any website under the domain name *mbna.co.uk*, or any other domain name incorporating the acronym "mbna" and (ii) prohibiting him from selling, offering for sale or otherwise dealing with the

*mbna.co.uk* domain name pending full trial.

MBNA claimed that the balance of convenience lay in granting injunctions in its favour pending full trial. The Bank alleged that the defendant had deliberately chosen the letters "mbna" for his website in order to take advantage of the Bank's goodwill and thereby to increase the number of visitors to his site. It referred to the Court of Appeal's comments in *One In A Million* that, where a defendant intends to appropriate goodwill, there is no reason for the court to infer that such appropriation will not take place. The Bank maintained that it would suffer damage from the defendant's registration through losing customers; it claimed that a person who browsed the Internet and found only a "website pending" message under the disputed domain name would conclude that MBNA conducted no Internet business and would therefore take his or her business elsewhere.

The judge was not sympathetic to this argument. He noted that the defendant's proposed banner exchange business would not compete with MBNA's credit card and financial services businesses and was unwilling to deprive the defendant of the opportunity to commence his business as soon as possible. The judge also thought it unlikely that Internet users would believe that there was any link or connection between MBNA and the defendant.[24]

With this in mind, the judge concluded that, on the basis of the balance of convenience, he should not grant an interim injunction preventing the defendant from activating his site prior to full trial. However, he did grant an injunction preventing the defendant from selling or dealing with the domain name pending full trial, on the basis that he should not be allowed to profit from any enhancement of the value to the website caused by hits from browsers looking for the MBNA site if the domain name registration was subsequently found to have been improper.

### 3.2 Summary judgement

Where the case against a cybersquatter or on-line infringer is particularly strong, summary judgment may provide an appropriate means for disposing of the action without the need to take proceedings all the way to full trial. In summary judgment proceedings, the court may be asked to give judgment on the claim on the basis of a limited amount of evidence and after a much shorter hearing.

Broadly speaking, an application for summary judgment can be made at any time after the defendant has filed his acknowledgement of service or defence.[25] It can be made on the whole of a claim or on a particular issue and by the claimant or defendant. It is possible for the court to grant summary judgment in the absence of the defendant.

The test for succeeding requires the applicant to show that:

(i) the other side has "no real prospect" of succeeding; and

(ii) there is no "other compelling reason" why the case should have to proceed to trial.[26]

In cases where the need for really urgent interim relief is marginal, but where the case on infringement is strong, it can be better these days to forego an interlocutory injunction and apply for summary judgment instead. The court processes have become so much quicker since the Woolf reforms that one can often achieve this end result in only a matter of a few weeks more than the time for obtaining an inter partes interlocutory injunction.

## 4. Remedies

A wide range of remedies are available in passing off and trade mark infringement proceedings, including: injunctions, declarations and damages or an account of profits.

A court can also order the defendant to transfer an impugned domain name registration to the claimant,[27] and/or grant an order for the obliteration on oath of any articles or documents (including the set-up and content of a website).[28] Registration authorities will be under an obligation to comply with all court orders relating to (non)use of domain names and their transfer.[29]

The extent of any damages granted will generally depend on whether (and if so, how much) quantifiable damage has occurred - for example, the costs of corrective advertising and/or losses caused by diversion of trade. Where the claimant is able to show damage to his goodwill in general terms (for example, by way of injurious association by the defendant or though dilution and/or loss of a reputation for excellence), some limited monetary relief may also be available.[30]

In addition, where there has been registered trade mark infringement, damages may be awarded on the so-called "user principle" i.e. to reflect the royalty that would have been payable for use of the mark with the owner's consent.[31] Damages are available on this basis even in the absence of a quantifiable monetary loss.

A successful claimant is also entitled to repayment by the defendant of the legal fees incurred in bringing an action. This entitlement may, however, prove to be somewhat theoretical, given that a cybersquatter will probably not have sufficient funds to pay all (or any) of the costs likely to have been incurred by a major brand owner.

## 5. What are the risks involved in starting proceedings?

Apart from the general risks inherent in all intellectual property and other litigation, there are two particular concerns relating to registered trade mark infringement claims of which a brand owner should always be aware.

### 5.1 Threats actions

Disgruntled trade mark owners should remember that the unjustified threat of a trade mark infringement action is actionable under section 21 *Trade Marks Act 1994* in the cybersquatting context as in any other form of trade mark infringement.[32]

Section 21(1) provides that, where a person threatens another with proceedings for infringement of a registered trade mark (other than in

relation to the application of the mark to goods or their packaging, the importation of goods to which, or to the packaging of which, the mark has been applied, or the supply of services under the mark) any "person aggrieved" may bring proceedings against the person making the threats. In the event that a favourable finding under section 21 is made, the court may give a declaration that the threats made were unjustifiable, may grant an injunction against further such threats and may award damages if the recipient has suffered loss as a result of the threats.[33]

In order to avoid an award under section 21, the person making the threats must show that the conduct complained of amounts (or would have amounted ) to infringement of the relevant marks.[34]

Whether a particular communication constitutes a threat is determined by looking at whether it would have been read by an ordinary reader, in the position of the recipient, as constituting a threat of infringement proceedings. Importantly, section 21(4) *Trade Marks Act 1994* provides that the mere notification that a trade mark is registered (or that an application has been made) does not constitute a threat of proceedings for these purposes.

Drafting a warning letter to a cybersquatter or other on-line infringer will involve striking a fine balance between simply notifying him of the existence of a brand owner's rights and conveying the desired message to the alleged infringer. As the courts have noted, a person who wishes to raise the possibility of infringement proceedings will be "required to take care in expressing himself".[35]

By way of illustration, it is instructive to consider the warning letter sent in the *prince.com* case. In this case, the court found that there had been threats by the claimant, as the warning letter sent by the claimant contained: an express reference to the claimant's trade mark registrations, a complaint about the defendant's use of the "prince" name which was unlimited in territorial scope and an unqualified requirement not to use "prince" as part of any new domain name. Most importantly, however, the letter finished with an entirely obvious threat of proceedings:

> *"... While we are willing to wait for your orderly transition to a new domain name, we must have your immediate written agreement to assign the PRINCE.COM name to Prince Sports to avoid litigation ... We look forward to hearing from you or your attorneys in the very near future".*

Brand owners should also note that a "veiled" threat is still a threat; it will not be possible to dilute an inference of threat by stating that no decision as to whether to bring proceedings has yet been reached or that a brand owner is simply "reserving its rights".[36]

### 5.2 Counter-claims by the alleged infringer

An additional risk in registered trade mark infringement cases is that of a counterclaim for revocation/ invalidation of the trade mark relied upon by the claimant (for example, on the basis of non-use or non-distinctiveness). A brand owner should always check the continuing validity of his rights before citing them in proceedings and opening them up to attack in this manner.

## C. Litigation in the United States

The US courts initially dealt with cybersquatting and other forms of on-line trade mark infringement through recourse to the US laws of trade mark infringement, unfair competition and trade mark dilution.[37]

As with the English laws of passing off and trade mark infringement, the application of existing rules to the new situations thrown up by the phenomenon of cybersquatting was not without its difficulties. In particular, US law (like English law) generally required that cybersquatters were shown to have sold or advertised some form of goods or services. A mere "blocking registration" of a domain name was generally unimpeachable.

The US courts were clearly aware of the limitations of the doctrines of trade mark infringement and dilution in cybersquatting cases:

> *"... it is clear that the new law was adopted to provide courts with a preferable alternative to stretching federal dilution law when dealing with cybersquatting cases."*[38]

In consequence, the US legislature intervened to create a new, statutory cause of action against cybersquatters. The *US Anti-cybersquatting Consumer Protection Act 1999* ("the ACPA") entered into force on 29 November 1999. Its effect is to strengthen the rights of US trade mark owners on the Internet. It does this by adding a new Section 43(d) to the *Lanham Act*, the existing US legislation on trade mark protection.[39]

### 1. Overcoming the jurisdictional hurdles - non-US defendants

### 1.1 The basic position

A full discussion of the US law relating to jurisdiction is outside the scope of this paper.[40] It is, however, essential to understand that the US treatment of jurisdiction is different to that of the English courts. Whether the US courts have jurisdiction over a particular defendant is essentially a question of whether that defendant has or has had "sufficient minimum contacts" with the US to satisfy the US constitutional due process requirements. A US court may also exercise jurisdiction over a foreign defendant where the defendant has "purposefully availed himself of the privilege of conducting activities in the forum", the damage complained of has arisen out of those activities and the exercise of jurisdiction by the US courts is considered to be "reasonable".

A number of US cases have considered jurisdiction in the Internet context and the basic position is as follows:

> *"The likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an*

*entity conducts over the Internet."*[41]

Hence, in Internet infringement cases, the question of whether there has been sufficient "minimum contact" will be decided on the basis of a three part sliding scale - from websites by means of which the alleged infringer "does business" over the Internet at the one extreme,[42] through interactive websites which permit a limited exchange of information,[43] to simple information-providing websites at the other.[44]

The purposive approach of the US courts to claiming jurisdiction over non-US defendants is well illustrated by a quotation adopted in the decision of the District Court of Illinois in *Euromarket Designs Inc - v- Crate & Barrel Limited*:[45]

*"[t]he United States has a substantial interest in regulating the conduct of business within the United States. ... By engaging in this commercial business, [the defendants] subject themselves to the in personam jurisdiction of the host country's courts. They waive either expressly or implicitly other objections that might otherwise be raised. A major reason for this subjection to business regulation is to place foreign corporations generally in the same position as domestic businesses."*[46]

### 1.2 In rem jurisdiction under the ACPA

The ACPA provides trade mark owners with a basic remedy *in personam* against cybersquatters. However, where the cybersquatter is anonymous, gave false details to the relevant registration authority or cannot be found, the ACPA also gives the trade mark owner the benefit of a new action *in rem* against the domain name itself.

New Section 43(d)(2) *Lanham Act* permits a trade mark owner to bring an action *in rem* against the disputed domain name itself if:

- the domain name violates a trade mark protected under the ACPA/*Lanham Act*; and
- it is not possible to obtain *in personam* jurisdiction over the registrant; or
- it is not possible (after a sufficient search) to locate the registrant.[47]

The *in rem* action should be brought in the judicial district of the relevant domain name registration authority.[48]

Although the relief available in an *in rem* action is limited (see section C(3) below), the *in rem* action available under the ACPA gives owners of trade marks protected in the US a considerable tactical and practical advantage over a non-US registrant who is alleged to be in breach of the ACPA. Defending proceedings in the US will be expensive and inefficient, yet any failure to submit to the jurisdiction of the US courts is likely to result in the US court ordering forfeiture of the domain name under the *in rem* provisions of the ACPA. Indeed, some case law applying the new in rem action suggests that a claimant does not need to first attempt to obtain personal jurisdiction over the defendant before making an *in rem* claim under the ACPA. This case law sits uneasily however, with the wording of the ACPA.[49]

## 2. The cause of action under the ACPA

The ACPA grants a civil remedy to a US trade mark owner (or the owner of a personal name protected as a mark) against any person who, with a "bad faith intent" to profit from that mark, registers, traffics in[50] or uses a domain name that:

- in the case of a distinctive mark, is identical or confusingly similar to that trade mark; or
- in the case of a famous mark, is identical or confusingly similar to, or dilutes, that trade mark.

The trade mark upon which a claimant under the ACPA relies need not be federally registered; the new Section 43(d) has been inserted in the part of the *Lanham Act* dealing with both registered and unregistered marks.

### 2.1 Bad faith

The distinctiveness of the complainant's trademark will be presumed if it is a US trade mark registration. There is no need to show a likelihood of confusion or dilution.

Establishing a "bad faith intent" on the part of the domain name registrant is crucial to liability under the ACPA. The ACPA contains a so-called "safe-harbour" provision, which states that "bad faith shall not be found in any case in which the court determines that the person believed and had reasonable grounds to believe that the use of the domain name was fair use or otherwise lawful".[51]

The ACPA contains a non-exhaustive list of factors for the US courts to take into account in considering whether there is a "bad faith intent" for the purposes of the ACPA. These include:

(i) any trade mark or other intellectual property rights belonging to the registrant in the domain name;

(ii) the extent to which the domain name consists of the legal name of the registrant or a name that is otherwise commonly used to identify the registrant;

(iii) any prior use of the domain name by the registrant in connection with a *bona fide* offering of any goods or services;

(iv) any *bona fide* non-commercial use of the trade mark by the registrant in the site accessible under the domain name;[52]

(v) evidence of the registrant's intent to divert consumers away from the trade mark owner's own website to the site established under the domain name, that could harm the goodwill represented by the trade mark, either for commercial gain or with the intent to tarnish or disparage the trade mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation or endorsement of the site;

(vi) any offer by the registrant to transfer, sell or otherwise assign the domain name to the trade mark owner or any third party for financial gain, without

having used, or having an intention to use, the domain name in the *bona fide* offering of goods and/or services and any pattern of such conduct;

(vii) the provision of false or misleading information by the registrant to the domain name registration authority and/or an intentional failure to maintain such accurate information and any pattern of such conduct;

(viii) the registration or acquisition by the registrant of multiple domain names which the registrant knows are identical or confusingly similar (in the case of distinctive marks) or identical or confusingly similar to or dilutive of (in the case of famous marks) the trade marks of third parties, without regard to the goods or services of those third parties; and

(ix) the extent to which the trade mark incorporated within the domain name is neither distinctive nor famous within the meaning of the Lanham Act.[53]

These factors are aimed at identifying redeeming or incriminating actions by the registrant. Hence (i) to (iv) and (ix) look for behaviour indicating the lawfulness of the registrant's conduct, while (v) to (viii) tend to indicate unlawful conduct.

Most notably, the absence of an offer by a cybersquatter to sell the disputed domain name will not be problematic if the trade mark owner can adduce evidence of a previous pattern of such offers. The blocking registration of multiple domain names is also caught by the ACPA.

### 3. Remedies

The US courts may order the forfeiture or cancellation of the domain name or the transfer of the domain name to the trade mark owner.[54] It may also grant injunctive relief, award damages, an account of profits and costs as in traditional trade mark infringement cases.[55] These remedies also lie against any authorised licensee of the cybersquatting registrant.

The ACPA allows trade mark owners to claim statutory damages (as an alternative to damages for actual loss or an account of profits) in cases involving domain names registered after the entry into force of the ACPA.[56] Statutory damages will vary between a minimum of $1,000 and a maximum of $100,000 per domain name as the court thinks just.

Relief in an *in rem* action is limited to an order for the forfeiture, cancellation or transfer of the domain name.[57]

### 4. Risks of commencing litigation

As in English litigation, there are some particular risks which may arise in the context of a cybersquatting claim. The ACPA provides that, if a domain name registration authority, acting upon a knowing and material misrepresentation by another person that a domain name is identical to, confusingly similar to, or dilutive of (as appropriate) a trade mark, cancels or transfers a domain name registration, the person who made the misrepresentation will be liable to the domain name registrant for any damages, costs and legal fees incurred by him/her and reactivation of the domain name or its transfer back to the registrant.[58]

Furthermore, even where the complainant is in the right, he/she is not entitled to recover the costs of the litigation.[59]

## D. Alternative dispute resolution – the UDRP

ICANN, the Internet Corporation for Assigned Domain Names and Numbers, adopted WIPO's proposals for a Uniform Dispute Resolution Policy ("UDRP") on 26 August 1999. The UDRP applies to the top level domains *.com*, *.net* and *.org* and came into operation on 1 December 1999.[60]

The UDRP is supplemented by rules of procedure adopted by ICANN on 26 August 1999 ("the UDRP Rules"), which provide guidance on the implementation of the UDRP. It can be characterised either as an inexpensive arbitration service for cybersquatting disputes or, perhaps more accurately, as an expert determination service.

Disputes arising from allegedly abusive registrations may be dealt with under the UDRP by filing a complaint with an approved dispute resolution service provider. Each dispute resolution service provider is obliged to follow the UDRP and the UDRP Rules, as well as any rules which it may have adopted itself.[61] The choice of dispute resolution service provider lies with the complainant.[62]

The first dispute resolution service provider accredited to administer the UDRP was WIPO.[63] It has been estimated that approximately 60% of the total complaints made under the UDRP have subsequently been filed with WIPO.[64]

### 1. Submission to the UDRP - overcoming the jurisdiction hurdle

The UDRP is incorporated by reference into the registration agreement between the domain name registrant and the registration authority.[65]

Submission to the UDRP does not preclude the submission of the dispute to any court of competent jurisdiction either prior to the commencement of the UDRP proceedings or after such proceedings are concluded.[66] Where a court action is commenced prior to or during a UDRP proceeding, the panel has a discretion to decide whether to suspend or terminate the UDRP proceeding.[67]

Submission of a complaint under the UDRP does however, preclude commencement of any court action against the relevant domain name registration authority.[68] The UDRP permits the consolidation of multiple disputes involving the same complainant into one proceeding.[69]

### 2. Basis of the complaint - "abusive registrations"

The UDRP is designed to tackle an "abusive registration" of a domain name. An "abusive registration" occurs if:

- the impugned domain name is identical or confusingly similar

to a trade mark or service mark in which the complainant has rights;[70]

- the registrant has no rights or legitimate interests in the domain name; and
- the domain name has been registered and is being used in bad faith.[71]

The complainant must show all three elements to succeed.

The protection offered by the UDRP applies to both registered and unregistered marks. The complainant must specify the basis for its complaint in respect of each of these criteria in its official complaint to the relevant dispute service provider.[72]

The UDRP Rules permit a Panel to apply any rules or principles of law that the Panel "deems applicable".[73] Panellists have clearly been willing to import such rules from both English and the US law.[74] In choosing this law, the Panel may be influenced by where the complainant and/or registrant are domiciled.

### 2.1 Confusing similarity

The UDRP does not provide any specific guidance on how confusing similarity is to be assessed. While it is generally accepted that the top-level country code is ignored for the purposes of comparison, there is wider difference of opinion as to how this test should be applied.

On the one hand, some Panellists have treated the assessment of confusing similarity as being entirely independent from any overall likelihood of confusion; they have undertaken a strict side-by-side comparison of the complainant's mark and the impugned domain name, looking only at broader issues such as whether a search engine would pull up the registrant's site if the complainant's name was typed in.

On the other hand, an assessment based more on the circumstances of the domain name registration (including its use, relevant products and the target market/users) has been advocated by some Panels.[75]

### 2.2 Legitimate interests in the domain name

Paragraph 4(c) of the UDRP sets out a non-exhaustive list of factors indicating a "legitimate interest" in a domain name. These include:

- evidence of use by the registrant or a demonstrable preparation to use the domain name, dating from prior to any notice from the complainant, in connection with the *bona fide* offering of goods or services;
- evidence that the registrant has been commonly known by the domain name, irrespective of whether he has acquired any trade mark or other rights in the name; or
- evidence that the registrant is engaged in a legitimate non-commercial or fair use of the domain name, without the intent to make commercial gain by misleadingly diverting consumers or tarnishing the trade mark or service mark upon which the claimant relies.

The claimant may also have a legitimate interest in a domain name where the mark upon which the complainant bases his case is descriptive or generic. A number of Panels have looked to US law to determine whether a name is sufficiently distinctive as to merit protection under the UDRP, applying the test of whether the name has a acquired a "secondary meaning in the relevant community" as a pre-condition to the right to take action.[76]

### 2.3 "Bad faith"

Although the claimant must prove all three elements of the "abusive registration" test set out above, the most important is that the domain name was registered and is being used in bad faith. It is important to remember that both registration in bad faith and subsequent use in bad faith must both be shown, although "use" can include the mere passive holding of a domain name.[77] The UDRP contains a non-exhaustive list of factors indicating bad faith on the part of the domain name registrant. These include evidence that the registrant:

- acquired the domain name primarily for the purpose of selling, renting or transferring the domain name to the complainant or a competitor of the complainant for more than the costs incurred by the registrant in registering the domain name;
- both registered the domain name in order to prevent the owner of the trade mark from using its mark in a corresponding domain name and has been engaged in a pattern of such conduct (as under the ACPA in US law, it is essential that a pattern of conduct can be shown to succeed on this basis);
- registered the domain name primarily for the purpose of disrupting the business of a competitor; or
- by using the domain name, has intentionally tried to attract users to his/her website by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation or endorsement of the registrant's website or goods and services.

## 3. Procedure under the UDRP Rules

Although it is the accredited dispute resolution providers who hear disputes under the UDRP, ICANN's UDRP Rules lay down the basic procedural structure for the process of the complaint.

### 3.1 The official complaint

The complainant must submit his complaint in both hard copy and electronic form under cover of a "Complaint Transmittal Coversheet".[78] Responsibility for forwarding the complaint to the alleged cybersquatter lies not with the complainant, but with the dispute resolution service provider (who is permitted a variety of means for this purpose, including e-mailing the registrant at the address as provided to the domain name registrar or simply e-mailing any active website found to be operating under the disputed domain name). The complaint must be forwarded within

3 days of receipt of the official fees from the complainant.[79]

The complainant has 5 days to rectify any errors or omissions in its official complaint which are notified to it by the dispute resolution service provider; failure to do so leads to the automatic without prejudice withdrawal of that particular complaint, but does not preclude the submission of a different complaint by the complainant.[80]

### 3.2 The timetable

The UDRP proceedings are deemed to commence on the date on which the dispute resolution service provider forwards the complaint to the registrant.[81] The registrant has 20 days thereafter in which to respond.[82] The panel is under a duty to ensure that the proceedings continue thereafter with "due expedition".[83] It should, in the absence of "exceptional circumstances", forward its decision to the dispute resolution service provider within 14 days of its appointment.[84] The dispute resolution service provider should then forward the decision to the parties within 3 days.[85]

The failure of the registrant to submit a response does not result in an automatic finding in favour of the complainant; rather, the panel must simply consider whether the necessary elements of the complaint have been made out in the case put forward by the complainant.[86]

It has been estimated that just over half of cases go uncontested.[87]

### 3.3 Proceedings of the panel

The panel has the discretion to decide what evidence is to be admissible and which legal rules and principles it considers applicable.[88] Generally, there are to be no oral hearings under the UDRP unless the panel considers it necessary.[89]

Decisions of three-member panels are reached by majority and all decisions must be given in writing.[90] Where a member of a three-member panel dissents, that dissenting opinion is attached to the decision.[91] The decisions are to be published on a publicly available website.[92]

A single panellist may determine a dispute. However, either the complainant or the respondent can elect to have the dispute decided by a three-member panel. The fees for a three-member panel are paid in their entirety by the complainant except where the respondent unilaterally requests three members, in which case the fees are shared equally.[93] WIPO's fees depend upon the size of the Panel and the number of domain name registrations in dispute in the complaint:[94]

| No. of domain names | Single Panellist (US$) | Three Panellists (US$) |
|---|---|---|
| 1 - 5 | 1,500 | 3,000 |
| 6 - 10 | 2,000 | 4,000 |

## 4. Remedies

If the complainant is successful, he/she is entitled to the cancellation or transfer to him/her of the disputed domain name.[95] These are the only two remedies available under the UDRP.

There are no interim remedies for the complainant; pending the outcome of the UDRP proceedings, the registrant is entitled to continue to use the disputed domain name.[96] Similarly, there is no final remedy equivalent to a permanent injunction or "cease and desist" order.[97] There are, however, restrictions upon the registrant's right to transfer the domain name pending the outcome of the dispute.[98]

WIPO has endorsed a general policy of ordering the transfer of a domain name, rather than its cancellation, on the basis that the risk of the domain name being obtained by an entity other than the complainant during its period of cancellation would "frustrate the intention of the Uniform Policy".[99] Of 3,662 cases filed under the UDRP to 10 May 2001 (concerning a total of 6,467 domain names), there have been 2788 decisions rendered, ordering transfer of the domain name(s) in 2202 cases, cancellation in only 22, and rejecting the complaints in 545.

The UDRP does not provide for the award of monetary compensation and a complainant will not be able to obtain damages or recover his costs in bringing the UDRP proceedings. A court action will, therefore, remain the more appropriate course of action where the claimant wishes to recover such damages or costs, although damages are often of more theoretical than practical interest in cybersquatting cases.

## 5. Risks involved in bringing a complaint

### 5.1 Allegations of reverse domain name hijacking

If a complaint is, in the view of the panel, brought in bad faith (for example, in an attempt to deprive a legitimate registrant of his name or to harass the registrant) the panel is entitled to make a declaration to this effect, stating that the complaint was an abuse of the UDRP proceedings.[100]

In order to make out an argument on this basis, the registrant must show that the complainant knew of the respondent's legitimate interest in the domain name or clear lack of bad faith, but nevertheless brought the complaint in bad faith.[101]

Findings of "reverse domain name hijacking" have been made by a number of UDRP Panellists. Typically, these have been made where the complainant has proceeded with the UDRP proceedings notwithstanding the submission of evidence by the registrant that indicates a legitimate interest in the domain name. Interestingly, however, some Panels have also found bad faith on the part of a complainant where he should have known (by making "reasonable" enquiries) that the registrant's interest was legitimate.[102]

In contrast, other Panellists have been unwilling to entertain reverse domain name hijacking claims in the context of a potentially legitimate dispute between the parties and have suggested that determination of such an issue would be a more appropriate matter for the courts.[103]

### 5.2 But no risk to trade mark registrations

It is generally established amongst UDRP Panellists that they have no jurisdiction to enquire into the validity or otherwise of a trade mark registration relied upon by the claimant. It will generally be

presumed that these are valid and subsisting. In any event, the UDRP Panel has no power to make any order which could require a trade marks authority to revoke or invalidate a mark.

## E. Alternative dispute resolution in the UK

Nominet UK introduced its current dispute resolution service ("the DRS") in 1997. This takes the form of a mediation policy which it operates in-house and through the Centre for Dispute Resolution ("CEDR"). However, Nominet UK is currently in the process of reviewing the DRS and intends to adopt an extensively reformed procedure as a result.[104]

### 1 The current DRS

The DRS has three stages:

(i) **Mediation or other commercial resolution** - Nominet UK will try to establish whether the parties can reach a mediated or commercial resolution to the dispute. It will contact the registrant of the disputed domain name and discuss possible resolution options, reminding the registrant of Nominet's powers to suspend or cancel the registration in appropriate cases.

(ii) **Decision by Nominet UK** - If the approach to the domain name registrant is unsuccessful, the dispute will move on to the second stage of the process. Nominet UK may suspend or cancel a domain name where it decides (*inter alia*) that the name is being used in a manner likely to cause confusion to Internet users or where legal action has commenced regarding use of the name. A written copy of the decision must be provided by Nominet UK to both parties.

(iii) **Expert determination** - If either party is unhappy with Nominet UK's decision, the proceedings move on to the third and final stage. The case is referred to an independent expert for review, who may hear additional argument from the parties. The expert will issue a written recommendation to Nominet UK either confirming or revoking the decision. However, Nominet UK is not bound by the expert's recommendation.

Mediation is a process by which the parties are encouraged to reach an acceptable compromise; it does not result in an independent determination of the merits of the parties' respective cases and Nominet UK expressly disclaims any entitlement to reach such a determination. The outcome of a mediation is only binding upon the parties if a mutually acceptable contractual settlement can be reached.

The English courts have declined to treat the Nominet DRS as a form of binding arbitration and will not stay court proceedings pending the outcome of the Nominet UK mediation.[105] The DRS has been criticised for this weakness.[106]

The DRS has also been criticised for favouring cybersquatters. By requiring actual use of the name and by making no provision for bad faith registrants, Nominet UK currently does not intervene against those who purchase a domain name and then put it up for auction. This contrasts with the approach of the UK and US courts and the UDRP.

### 2 Proposed changes

The proposed new system aims to introduce a refined set of criteria to control abusive registrations, to retain the in-house mediation service and to provide for initial as well as appealed decisions to be rendered by independent experts. It will also be possible for a domain name to be transferred to a successful claimant, an important remedy not included in Nominet UK's current process.

Although these changes should bring Nominet UK's procedure more in line with the current thinking, the proposals as they currently stand contain a number of important flaws.

#### 2.1 The revised test to be applied by Nominet UK

The proposed set of criteria moves away from the current test of "likelihood of confusion to Internet users". Instead, it will require the claimant to show:

(i) on a balance of probabilities, that it has rights in a name or mark which is identical or similar to the domain name in dispute; and

(ii) beyond reasonable doubt, that there has been bad faith registration and/or use of the domain name by the registrant.

#### 2.1.1 Standards of proof

Although acknowledging the success of the UDRP procedure for tackling bad faith registrations, Nominet UK believes the UDRP system to be biased in favour of complainant brand owners. It is for this reason that it proposes adopting the criminal standard (of "beyond reasonable doubt") for proving bad faith. This has, however, been strongly criticised on the basis that it will give the domain name registrant too great an advantage over the brand owner. The criminal standard is also inappropriate in an informal paper-based resolution process and imposes a greater evidential burden on complainants than would be the case in court proceedings.

#### 2.1.2 Showing bad faith

Nominet UK has suggested the following non-exhaustive list of factors suggestive of bad faith, namely:

(i) any evidence that the registration was made:

(a) primarily for the purpose of transferring the domain name to a competitor or to the complainant for valuable consideration in excess of the out-of-pocket costs directly associated with acquiring or using the domain name; or

(b) as a blocking registration against a name or mark in which the complainant has rights;

(c) primarily for the purpose of disrupting the business of the complainant; or

(ii) any evidence that the domain name is being used in a way

that has confused others into thinking it to be registered to, operated or authorised by or otherwise connected with the complainant.

There is also a proposed non-exhaustive list of ways in which a registrant may prove an absence of bad faith. For example, the registrant may try to show that, prior to the claimant's notification, he had :

- used or made use of the domain in connection with a genuine offering of goods or services; or
- been commonly known by the same name or legitimately connected with a mark identical or similar to the domain name; or
- made legitimate non-commercial or fair use of the domain name.

The registrant may also argue that the domain name is generic or descriptive.

### 2.2 Revised procedure

From the initial complaint the registrant will have 15 working days to respond and the claimant will have a further 5 days to reply. There will then be a 10 day period during which Nominet UK will offer a free mediation service along the current lines. After the expiry of this period, the case is referred to an independent panellist, chosen on a cab rank (i.e. rotational) basis from a list of Nominet UK appointees. The aim is to have a decision available 10 days from the panellist's appointment.

All of these time limits can be extended at Nominet UK's (or the panellist's) discretion. (As some practitioners have noted, the 5 day reply period will rarely be sufficient to permit a brand owner to consider its position and to give instructions to its legal representatives.)

Dissatisfied parties can appeal the decision to a panel of 3 independent experts drawn from the same list. As under the UDRP, the parties can at any time refer the matter to court for resolution, in which case Nominet UK has a discretion to suspend its own dispute procedure.

### 2.3 Risks involved in bringing a claim - "three strikes you're out"

The new Nominet procedure currently contains a provision by which complainants may be prevented from bringing further proceedings under the Nominet process. If the adjudicating expert(s) make a finding that complaints have been brought in bad faith on 3 separate occasions by a particular complainant, Nominet UK will then accept no further complaints from that entity. The criteria by which a finding of bad faith may be made have not been set out in detail by Nominet UK.

This part of the proposal has been criticised as overly harsh on brand owners. While there is a legitimate concern to avoid abuse of the system by complainants, the system should not deter complainants from pursuing cybersquatters where they believe they have a genuine grievance. However, there is of course the option for a complainant from seeking remedies through the courts.

## F. Word-Stuffing, Mousetrapping, Spamming and more

Just as the law begins to catch up with illegitimate activities on the Internet, so new and more novel ways of using and abusing brand names are discovered.

To illustrate the differences between the approaches of, and causes of action available in, the English courts, the US courts and under the UDRP, this paper concludes with a review of a few of the more inventive types of Internet infringement to have recently emerged.

### 1. Wordstuffing and meta-tags

Meta-tags are the key words, contained in the HTML source code of a website, which are used to describe the contents of the site. Meta-tags are picked up by search engines and are used by the search engines to direct Internet users to particular sites when surfing the Internet. The meta-tags on a site are invisible to the user (although they can be viewed in Netscape by using the View/Source options).

"Word-stuffing" describes the practice of including as much information as possible in a website's meta-tags. By increasing the scope of the meta-tags, more users should be diverted to a website by search engines. Irrespective of whether the user then trades on that site, it is often the case that a mere "hit" alone can increase the value of a domain name registration for advertising revenue purposes.

Recent case law in the US and UK has highlighted the practice of setting up meta-tags containing a competitor's trade marks, in order to divert users who type in those brand names when using search engines. This process has also been described as "bait and switch" as it operates, to a certain extent, in the hope that a user will decide to use the site he reaches, rather than the one he was originally looking for.

There is now a clear line of authority in the US that this type of conduct will amount to trade mark infringement.[107] In reaching this position, the US courts have relied upon the concept of "initial interest confusion" - in other words, the confusion experienced by an internet user when he ends up on a website which he/she did not expect.[108] The US courts have recognised that, although users will realise that the site they have reached is not that of the claimant, they may nonetheless decide to use the defendant's services instead.

The issue has now also been considered by the UK courts. In *Roadtech Computer Systems -v- Mandata*,[109] the court held that the claimant was entitled to summary judgment on the basis of both passing off and registered trade mark infringement arising out of the use of its trade marks in a competitor's meta-tags. As the defendant admitted liability for registered trade mark infringement, the court did not consider this claim in detail. In terms of passing off, however, the court held that use of the marks in the meta-tags amounted to a false representation by the defendant to Internet users looking for the

claimant or its products using search engines that the defendant's site or the goods/services it advertised were in some way linked to the claimant.

Although this decision is not of great authority in terms of precedent (it is the decision of a Master, not a judge), it indicates that the English courts are likely to take an approach similar to that of the US courts. As the court stated:

> *"this was a deliberate, albeit unsophisticated appropriation of the claimant's rights for which some compensation ought undoubtedly to be paid".*[110]

Even where a claim primarily concerns the disputed registration of a domain name, the appropriation of meta-tags by the registrant may be treated by the English courts in passing off claims as evidence both of the value of the claimant's goodwill and of the defendant's intent.[111]

A similar approach has also been taken by WIPO Panellists. Although the UDRP does not empower a Panel to consider the practice of word-stuffing in isolation,[112] this conduct has repeatedly been accepted as "most potent evidence of bad faith" on the part of the domain name registrant.[113]

### 2. Invisible wording and concealed banners

Web browsers do not always search for relevant sites by looking at the meta-tags alone. Instead, a search engine will also often search against the text on the front page of a website for relevant references.

The defendant in the *Roadtech* case included his competitor's marks not only in the meta-tags of his site, but also on his home page. The marks were included in a typeface which was the same colour as the home page background, so that they were invisible to users. Not surprisingly, the court in *Roadtech* also considered this to amount to passing off and registered trade mark infringement.

### 3. Pagejacking and mouse-trapping

"Pagejacking" refers to the practice of copying webpages and applying them to newly set-up websites under pretence that the site is the genuine, copied site. This is usually combined with the registration of a domain name which is only minutely different to that of the genuine website (for example, by using a slight misspelling). The copied webpages are then re-submitted to search engines in order to divert users.

Pagejacking has a number of possible uses. For example, the number of hits on the copied site may increase the value of the domain name registration. Alternatively, it can be combined with "mouse-trapping". This involves routing a user who accesses the fake site through a number of (inescapable) links, for example, advertising the registrant's products, before the registrant is able to leave the site. In one extreme case, the US Federal Trade Commission took action against an individual who copied approximately 25 million webpages in order to feed users through his pornographic sites.[114]

While copying the original webpages will amount to copyright infringement, there is some US authority for the proposition that pagejacking and mouse-trapping may give rise to a cause of action under the ACPA when combined with the "abusive registration" of a domain name.[115]

Pagejacking and mouse-trapping have also been considered under the UDRP. In *Dow Jones & Company -v- John Zuccarini,*[116] the Panel considered that the use of the domain names wallstreetjounal.com and wallstreetjournel.com to feed users through a succession of advertisement links set up by the registrant was a clear indication of bad faith.

### 4. UBE and spamming

The sending of unsolicited bulk e-mails (sometimes called "UBE" or "spam") has become a significant problem for Internet users. Although internet service providers have developed software designed to filter out spam e-mails, this software is not always effective. In particular, bulk e-mailers have developed software which allows them to superimpose false headers on the e-mails sent, thereby hiding the identity of the real author of the message and the message's transmission path. These false headers will typically include non-existent email addresses.

There is now a clear line of authority in the US to the effect that the sending of spam e-mails which contain a third party brand name may amount to trade mark infringement under the *Lanham Act.*[117] In particular, using a false e-mail address ending with the domain or brand name of a third party (such as *aol.com*) has been considered by the US courts as making it appear that the messages are sent with at least the tacit approval of the third party concerned.

The sending of spam e-mail has also been treated as evidence of "bad faith" on the part of a domain name registrant under the UDRP.[118]

### 5. "Sucks" websites

A final point for any brand owner to consider is the extent to which it is protected against critics who register domain names incorporating its brand name in combination with derogatory terms. The most common examples of this are so-called "sucks" websites.

Interestingly, the US courts and UDRP Panels have adopted extremely different stances with regard to "sucks" domain name registrants.

On the one hand, the US courts have generally taken the view that use of a trade mark in conjunction with "sucks" in a domain name and/or on a "sucks" website is not trade mark infringement. Instead, the US courts treat this as a form of non-commercial expression which is covered by the First Amendment of the US Constitution, protecting freedom of speech.[119] As such, it also falls within the "safe harbour" fair-use provisions of the ACPA.[120]

On the other hand, UDRP Panels have tended to treat "sucks" domain names as liable to transfer or cancellation under the UDRP.[121] This conclusion involves findings

both of bad faith on the part of the registrant and, more controversially, a confusing similarity between the brand name on its own and the version combining it with "sucks". In a number of UDRP decisions, the Panel has rejected the argument that the "sucks" element of the domain name makes clear that the registrant and brand owner are not linked:

> *"... can it be said that the registration would be recognised as an address plainly dissociated from the Complainant? In the Panel's opinion, this is by no means necessarily so. The first and immediately striking element of the Domain Name is the Complainant's name. Adoption of it in the Domain Name is inherently likely to lead some people to believe that the Complainant is connected with it. Some will treat the additional "sucks" as a pejorative exclamation and therefore dissociate it after all from the Complainant; but equally others may be able to give it any very definite meaning and will be confused about the potential association with the Complainant".*[122]

Panels have also been influenced by the facts that "sucks" is an English language slang word which may not be understood by non-English speaking users of the Internet and in relation to which the negative connotations may not, therefore, be readily apparent.

These UDRP decisions have been the subject of considerable criticism by commentators and certain Panellists have taken an approach more in line with US authority.[123]

## G. Conclusion

This paper would not be complete if it failed to recognise that a large proportion of cybersquatting and other Internet trade mark disputes are settled without the need for either court or UDRP proceedings. Cybersquatters, in particular, are aware that brand owners are often prepared to spend at least as much as double the UDRP Panel fees for an agreed outcome, rather than risk losing the dispute. As in any other settlement situation, the amount that the brand owner is prepared to pay will depend on the value of the brand concerned, the perceived damage to the brand owner's goodwill from the existence or use of the infringing domain name, the merits of the case and the cost to the brand owner of pursuing the cybersquatter through the courts or a dispute resolution process.

Having said that, it is worth remembering that, in cases where the UDRP applies, and where there is good evidence of bad faith, it can be significantly cheaper to use the UDRP than to pay lawyers to negotiate with a cybersquatter.

The UDRP has been widely hailed as a success - a quick and relatively inexpensive method of stamping out cybersquatting which avoids the need for litigation in the courts. It is clear from the statistics that UDRP panels are taking a tough line against cybersquatters: approximately 80% of cases determined through WIPO have to date resulted in a decision in favour of the complainant.

However, the UDRP system is not without its flaws. Most importantly, UDRP proceedings are narrowly defined in scope. As a result, there may well be certain disputes which give rise to issues wider than simple "bad faith" registration/use upon which a UDRP Panel will not have jurisdiction to opine. As a number of WIPO Panellists have noted, there will always be certain "legitimate disputes" (such as trade mark invalidity) which are suited more for resolution by national courts than under the UDRP. It is for this reason that the UDRP provides that the parties to a UDRP proceeding are free to pursue other available remedies if they are not happy with the Panel's decision.[124]

In addition, the limited remedies available will mean that a UDRP decision cannot provide complete protection/compensation where the brand owner has suffered loss or where registration of the disputed domain name is not the only issue at stake. Even when a domain name registration is transferred under the UDRP, the content of the site, the links and the meta-tags can all be moved by the registrant to another address.

In short, while the UDRP can always be treated as a first "port of call" in *.com* cases, it is not possible to rule out the fact that a brand owner may ultimately need to have recourse to the courts. In any event, as far as *.co.uk* domains are concerned, litigation is likely to be the only effective course of action until the Nominet DRS has been amended.

---

* **Authors' acknowledgements**: The authors owe their thanks to **Michael Metteauer** of Fulbright & Jaworski, who reviewed an earlier draft of the US law section and made many useful suggestions for improvement.

1 For the purposes of this paper, the term "cybersquatting" is used to refer to the registration in bad faith of a domain name containing the trade mark of a third party; "on-line infringement" is intended to encompass all other forms of wrongful use of a trade mark on the Internet.

2 This applies to all EU states and was extended to cover EFTA states by the Lugano Convention 1988.

3 Rule 6.19 Civil Procedure Rules.

4 Articles 2 and 5(3) Brussels Convention 1968.

5 Article 16(4) Brussels Convention 1968. Where proceedings have been started abroad, Article 19 Brussels Convention 1968 operates to bring such cases back into the English courts.

6 Rule 6.21 Civil Procedure Rules.

7 Depending on the circumstances, other forms of intellectual property right may also be relevant. For example, a registrant may copy text and other material from the brand owner's website or may create unauthorised links to that site, thus potentially giving rise to a claim for breach of copyright. The availability for relief for copyright infringement and other forms of intellectual property infringement are outside the scope of this paper.

8 *British Telecommunications Plc -v- One In A Million Ltd and Others; Virgin Enterprises -v- One In A Million Ltd; J Sainsbury Plc -v- One In A Million Ltd; Marks & Spencer Plc -v- One In A Million Ltd; Ladbroke Group Plc -v- One In A Million Ltd* (consolidated) [1999] FSR 1. The disputed domain names included *marksandspencer.com, marksandspencer.co.uk, sainsbury.com, j-sainsbury.com, virgin.com, bt.org* and *ladbrokes.com*.

9 *Per* Jonathan Sumption QC at first instance in *One In A Million*, quoted with approval by the Court of Appeal.

10 [1980] RPC 31, otherwise known as the *Advocaat* case.

11 A quia timet action is one in which the claimant bases his claim upon the threat of

damage in the future, rather than on actual damage suffered prior to the commencement of the claim.

12 It should always be remembered that this extension of the doctrine of passing off will apply in all contexts, not just cybersquatting. It may, for example, be particularly useful where a third party registers company names which would otherwise have been sought by a brand owner (as was the case in *Glaxo Plc -v- Glaxowellcome Ltd* [1996] FSR 388).

13 The judge said that "marksandspencer.com" was an inherently deceptive domain name. However, the other registrations, for example "ladbrokes.com" and "sainsbury.com", were not inherently deceptive, as other businesses or individuals might have corporate names or surnames which included these words.

14 Recent successful claimants include Britannia Building Society (*Britannia Building Society -v- Prangley,* Chancery Division 12 June 2000) and easyJet (*easyJet Airline Co Ltd -v- Tim Dainty*, Chancery Division 19 February 2001). Although easyJet won its case, the *easyJet* decision illustrates the requirement for a distinctive name. The case concerned the domain name registration easyRealestate.co.uk and a website which had been set up under that domain, using designs very similar to those of the logos of the easyJet group of companies. Noting the fact that there was no overlap between the activities of claimant and defendant, the judge was most influenced by the fact that the defendant appeared to have deliberately copied the claimant's logos and its "distinctive" orange livery. There was, therefore, a similarity between the claimant's and defendant's websites which was "suggestive of association". The judge did not consider "easyJet" or the prefix "easy-" to be names inherently leading to passing off; in the absence of the copying of the easyJet "get-up", it is unlikely that the claimant would have succeeded. Unsuccessful claimants have included French Connection (*French Connection Ltd -v- Sutton* (2000) ETMR 341) and MBNA America Bank (see section (B)3.1 of the main text below).

15 *Reddaway -v- Banham* [1896] AC 199: "[t]he name of a person or words forming part of the common stock of language may become so far associated with the goods of a particular maker that it is capable of proof that the use of them by themselves without explanation or qualification by another manufacturer would deceive a purchaser into the belief that he was getting the goods of A when he was really getting the goods of B".

16 *eFax.com Inc -v- Oglesby* [2000] Masons CLR 28. This judgment concerned an application for an interim injunction and a counter-application for summary judgment against the claimant. See Case Comment in PLC, March 2000 and Csaky "Round-up of Recent Case Law Related to IP and the Internet", Corporate Briefing March 2000.

17 *Lawyers Online Limited -v- Lawyeronline Limited* (7 July 2000, Judge Boggis QC).

18 The claims of registered trade mark infringement were not the subject of the summary judgment application which formed the basis of the appeal of *One In A Million* to the Court of Appeal (although the Court of Appeal did consider certain questions relating to registered trade mark infringement *obiter*).

19 Section 10 Trade Marks Act 1994, drawing from Article 5 First Council Directive (89/104/EEC).

20 *1-800 Flowers Inc -v- Phonenames Ltd* [2000] ETMR 369 and *Euromarket Designs Inc -v- Peters* [2000] ETMR 1025. He also noted that there was great need for ECJ authority on this issue (see *Euromarket*).

21 Section 46(1) Trade Marks Act 1994.

22 [1975] AC 396.

23 Nicholas Strauss QC, Chancery Division 17 July 2000.

24 This view is similar to that of Rattee J in *FCUK*, who noted that it would only take a "fraction of a second" for an Internet user to conclude that the sites of the claimant and defendant in that case were unconnected.

25 Rule 24.4 Civil Procedure Rules.

26 Rule 24.2 Civil Procedure Rules.

27 See, by way of illustration, *One In A Million* (footnote 8 above) and *easyJet* (footnote 14 above). This has been equated in conceptual terms to an order for delivery up (Jonathan Sumption, *One In A Million*).

28 See *Roadtech -v- Mandata* (section (F)1 of the main text below) and *easyJet* (footnote 14 above).

29 See *Marks & Spencer plc -v- Craig Cotterel and Others* (Chancery Division, 26 February 2001). Interestingly, the judge in this case thought that it should not "be assumed by domain name providers that they have no responsibility to monitor whether court orders prohibiting use, not merely of particular names, but also of colourable imitations are being broken by registrations made with the names which fall foul of the prohibition". However, he did not go further on this topic, stating that it was a difficult question requiring detailed argument.

30 *Harrods -v- Harrodian School Ltd* [1996] RPC 697, considered in *easyJet*. However, on the facts of the *easyJet* case, the judge ruled that there was no basis for an award of damages under this head.

31 In the *Roadtech* case (footnote 109 below), the court awarded £15,000 on this basis. The judge was clearly influenced by the fact that the defendant had "taken a ride on the back of" the claimant's site.

32 See, for example, the decision in the *prince.com* case (*Prince plc -v- Prince Sports Group Inc* [1998] FSR 21).

33 Section 21(2) Trade Marks Act 1994.

34 Section 21(3) Trade Marks Act 1994.

35 See *prince.com* (footnote 32 above).

36 *L'Oreal (UK) Limited and Another -v- Johnson & Johnson and Another* [2000] ETMR 691.

37 An established or famous trade mark is "diluted" within the meaning of the US Federal Trademark Dilution Act 1995 if it is tarnished or blurred by the mark adopted by the defendant. The US courts went so far as to hold that "internet cyberpiracy constitutes *per se* trade mark dilution" (*Virtual Works, Inc. -v- Network Solutions, Inc.* 54 USPQZd 1126).

38 *Sporty's Farm LLC -v- Sportsman's Market, Inc, US Court of Appeals* (2 February 2000).

39 The Trade Mark Act of 1946 (as amended) 15 USC section 1125(d). The existing US doctrines of trade mark infringement, unfair competition and trade mark dilution continue to apply to on-line infringement (ie. non-cybersquatting ) cases.

40 For a useful and more detailed discussion of this issue see Martin B Schwimmer, "Closing in on 'Target': The Internet and Personal Jurisdiction" (C.W. 1999, 90 Supp May 1999, 17-21).

41 *Zippo Manufacturing Co -v- Zippo Dot Com Inc*, 952 F Supp at 1124.

42 "If the defendant enters into contracts with residents of a foreign jurisdiction ... over the Internet, personal jurisdiction is proper" (*Zippo*).

43 In *Maritz, Inc -v- Cybergold, Inc* (947 F Supp 1328) the court found personal jurisdiction on the basis that, although the defendant's website was not fully operational, it was possible for a user to leave details on a mailing list: this was "clearly intended as a promotion ... and solicitation ... suggesting that the defendant [was] purposefully availing itself of the privilege of conducting activities [in the forum state]".

44 "A passive web site that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction" (*Zippo*).

45 96 F Supp 2d 824. This litigation proceeded in parallel with the UK *Euromarket* case (see footnote 20 above).

46 A quotation from *Laker* (731 F 2d at 924-5). It is interesting to note that, whereas Jacob J in *Euromarket* reached the conclusion that there was no use of the claimant's marks in the UK on which to found an action for registered trade mark infringement under English law, the US court, considering the same facts, concluded that there had been sufficient activity in the US to give the court jurisdiction over the defendants notwithstanding the parallel litigation in Ireland at the time.

47 The trade mark owner can show that he has made a sufficient search for the registrant by sending a notice of the alleged infringement and the intent to take action under Section 43(d)(2) to the registrant at both his postal and e-mail

addresses as provided to the domain name registration authority and by publishing a notice of the action as directed by the court after filing the action (new Section 43(d)(2)(A)(ii)(II) Lanham Act). These actions also constitute service of process (new Section 43(d)(2)(B) Lanham Act).

48 New Section 43(d)(2)(A) Lanham Act.

49 In *Caesars Word Inc v Caesars Palace.com and others* (District Court of Virginia, 8 March 2000) the defendants argued that the claimant could not bring an *in rem* action until it had attempted, and failed on the basis of a successful jurisdictional challenge, to bring an action *in personam* against them. This argument was rejected by the court on the basis that, since the defendants were in any event resisting the jurisdiction of the US courts, any action *in personam* would be "fruitless and a waste of resources". The court also rejected the argument that Section 43(d)(2) ACPA is unconditional *per se*.

50 "Trafficking in" a trade mark encompasses selling, purchasing, lending, pledging, licensing and any other transfer for consideration or receipt in return for consideration.

51 New Section 43(d)(1)(B)(ii) Lanham Act.

52 Setting up a non-infringing website (for example, a blank screen) under the disputed domain name will not, however, permit the registrant to escape from the ACPA if he fulfils other criteria relevant "bad faith" criteria. This rule, developed in *Panavision International -v- Toeppen* 141 F.3d 1316, was expressly stated by the Senate to be unaffected by the introduction of the ACPA.

53 Defined by Section 43(c)(1) Lanham Act.

54 New Section 43(d)(1)(C). This is in line with the existing US case law on remedies against cybersquatters.

55 Amended Sections 34(a) and 35(b) Lanham Act.

56 New Section 35(d) Lanham Act. As mentioned in the main text (above), the ACPA came into force on 29 November 1999.

57 New Section 43(d)(2)(D) Lanham Act.

58 Section 32(2)(D)(iv) Lanham Act.

59 This differs from the position in English law, where the successful brand owner will be entitled to recover a substantial proportion of his costs.

60 The UDRP does not apply to national top level domains such as *.fr* or *.es*, although ICANN hopes to extend its operation in future. For example, it is thought that the UDRP will be applied to the new *.eu* top level domain name and a similar policy to be introduced in the People's Republic of China.

61 For example, WIPO's supplemental rules are available on WIPO's website. The differences between each provider's rules may be importance; for example, the National Arbitration Form is the only provider whose rules give the complainant an automatic right to reply to the respondent's defence.

62 Paragraph 4(d) UDRP.

63 WIPO obtained formal approval from ICANN on 29 November 1999. There are three other approved dispute resolution providers: the CPR Institute for Dispute Resolution (US), Disputes.org/eResolution Consortium (Canada) and the National Arbitration Forum (US).

64 See Mutimear "UDRP puts pressure on cybersquatters" (Managing Intellectual Property, December 2000/January 2001).

65 Paragraph 1 UDRP. For example, the pro forma registration agreement for Network Solutions Inc incorporates by reference a domain name dispute resolution policy which was approved by ICANN on 24 October 1999; this policy in turn incorporates the UDRP by reference and reproduces a number of its provisions.

66 Paragraph 4(k) UDRP. Orders for the transfer or cancellation of a domain name made under the UDRP will not be put into effect if, within a period of 10 days from the date of the decision, the relevant UDRP panel receives notice and official documentation (such as a claim form) showing that the dispute has been submitted to court by the cybersquatter in a jurisdiction to which the complainant has submitted (the UDRP Rules require a complainant to submit to the jurisdiction of the courts of the relevant registration authority or the address of the domain name registrant as a pre-requisite to filing a complaint under the UDRP: UDRP Rules, paragraph 3(b)(xiii)).

67 Paragraph 18 UDRP Rules.

68 Paragraph 3(b)(xiv) requires an undertaking to this effect from the complainant; this undertaking also applies to the administrative panel (with an exception for "deliberate wrongdoing") and ICANN. The UDRP itself also contains an undertaking on the part of a domain name registrant not to join the relevant domain name registration authority as a party in any court proceedings (Paragraph 6).

69 Paragraph 4(f). This provision was used, for example, in an action brought by Alta Vista against a company which had registered over thirty variations of the Alta Vista name (WIPO, D2000-0848).

70 The complainant is required to describe, in his official complaint, the trade marks or service marks upon which its complaint is based and the goods and services for which it is used; the complainant is also allowed to adduce evidence of any goods or services in relation to which it intends to use the mark at some time in the future: paragraph 3(b)(viii) UDRP Rules.

71 Paragraph 4(a) UDRP.

72 Paragraph 3(b)(ix) UDRP.

73 Paragraph 15 UDRP Rules.

74 For example, in the *Jeanette Winterson* case (WIPO D2000-0235), the Panel looked to English law for principles which would have permitted the author to take action against unauthorised use of her name in the absence of a trade mark registration. The Panel had no doubt that, in line with the common law principles developed in *One In A Million*, she would have had at least a theoretical action for passing off. This was sufficient right upon which to base a complaint under the UDRP. The Panel did not, however, go so far as to apply *One In A Million* to see whether passing off had or might take place.

75 For example, compare *Gateway Inc -v- Pixelera.com Inc* (WIPO, D2000-0109) to *Yahoo! Inc -v- Eitan Zviely* (WIPO, D200-0273) discussed by Solomon ("Two New Tools to combat Cyberpiracy - A Comparison, The Trademark Reporter Vol 90 September-October 2000).

76 See for example *Pet Warehouse -v- Pets.Com Inc* (WIPO, D2000-0105) and *Los Angeles County Bar Association -v- JD Barnett Law Offices* (NAF FA00011000096113).

77 Provided that at least one of the other elements of bad faith is present (see *Telstra Corporation -v- Nuclear Marshmallows*, D2000-00003).

78 UDRP Rules, paragraphs 3(a) and 3(b)(xii); the form of the Complaint Transmittal Coversheet may be determined by each dispute resolution service provider (WIPO's version is available on its website, see part (H) below for details).

79 UDRP Rules paragraphs 2(a) and 4(a).

80 Paragraph 4(b) UDRP Rules.

81 Paragraph 4(c) UDRP Rules.

82 Paragraph 5(a) UDRP Rules. This period is extendable at the discretion of the dispute resolution service provider: paragraph 3(d) UDRP Rules.

83 Paragraph 10(c) UDRP Rules.

84 Paragraph 15(b) UDRP Rules.

85 Paragraph 16 UDRP Rules.

86 Paragraph 3(e) UDRP Rules.

87 David Tatham, "The Internet and the Universal Domain Name Dispute Resolution Policy", a paper delivered at a seminar of the Intellectual Property Institute on 12 December 2000.

88 Paragraphs 10(d) and 15(a) UDRP Rules: see also footnote 74 above.

89 Paragraph 13 UDRP Rules.

90 Paragraphs 15(c) and (d) UDRP Rules.

91 Paragraph 15(e) UDRP Rules.

92 Paragraph 16(b) UDRP Rules. Decisions may currently be viewed on the ICANN website (see part (H) below).

93 Paragraph 6(c) UDRP Rules.

94 As at 15 May 2001.

95 Paragraph 4(i) UDRP.

96 This is a departure from the position under the dispute resolution policy operated by Network Solutions, Inc. prior to the introduction of the UDRP, which contained a so-called "on-hold" provision pending the decision on entitlement to the domain name.

97 *Sports Car World Inc - v- Malcolm Cracknell* (NAF FA94448 (2000)).

98. Paragraph 8 UDRP. These include restrictions on both transferring the domain name to another "owner" and to another registrar; the restrictions apply not only to UDRP proceedings, but also (with slight amendments) to any court action or arbitration.

99 Engelman "ICANN's new Uniform Domain Name Dispute Resolution Policy" (domain.news June 2000).

100 Paragraphs 1 and 15(e) UDRP.

101 *Sydney Opera House Trust -v- Trylynx Pt Ltd* (WIPO D2000-1224).

102 See, for example, *Goldline International Inc -v- Gold Line* (WIPO D2000-1151).

103 See *Chromalloy Men's Apparel Group Inc -v- Burch & Hatfield Formal Shops Inc* (WIPO, D2000-1046): "for the Panel to make such a serious determination would require further probing into the Complainant's motivations in initiating this proceeding. Such an inquiry might more appropriately be undertaken in a court setting".

104 The consultation process of the review is now closed and Nominet's response to the comments it has received are awaited.

105 See *Lawyers Online Limited -v- Lawyeronline Limited* (footnote 17 above).

106 It has, for example, been described as "some what naïve" (IT Bristows, Commercial Law Journal October 2000).

107 See, for example *Niton Corporation -v- Radiation Monitoring Devices* (27 F Supp 2d 102) and *Oppendahl & Larson -v- Advanced Concepts* (1998 US Dist LEXIS 18359).

108 Interestingly, there is authority for the proposition that "initial interest confusion" is not a sufficient basis for a trade mark infringement claim which concerns the mere act of domain name registration. As one commentator has observed, the US courts' approach to meta-tags may, however, be a policy decision reached in the light of the clear "predatory intent" of a wordstuffer and the advertising revenues which may be generated simply by hits (albeit hits made in error) against a site: see Dawn Osborne "Thumbs down for wordstuffing" (E-Commerce Law & Policy 2000).

109 [2000] ETMR 970.

110 [2000] ETMR 970, per Master Bowman

111 See *Lawyers Online Limited -v- Lawyeronline Limited* (discussed at section (B)2.1.4 above) in which the judge said: "It is also significant in coming to [the conclusion that there was goodwill in the name] that the defendant caused Lawyers Online to be listed in a meta-tagging system which was set up. I am told that this was entirely by error and was an innocent mistake. But it just goes to show the importance of the name and the way in which that mistake could happen".

112 *Rollerblade Inc -v- CBNO and Another* (WIPO, D2000-00427).

113 See *DeRisk IT Ltd -v- DeRisk IT Inc* (WIPO, D2000-1288). Other examples include: *World Wrestling Foundation Entertainment, Inc -v- Aaron Rift* (WIPO, D2000-1499 and *Walmart Stores Inc -v- Walsucks and Walmart Puerto Rico* (WIPO, D2000-0477).

114 *Federal Trade Commission -v- Pereira* (US District Court of Virginia, 20 September 1999).

115 *Shields -v- Zuccarini* (US District Court of Pennsylvania, 89 F Supp 2d 634).

116 WIPO, D2000-0578 (the case involved the same Mr. Zuccarini as in the US litigation above; this practice appears to have been very profitable as his "click-based" advertising revenues were described by the US courts as in the region of $1 million a year).

117 A large number of these decisions have involved America Online Inc (AOL): see *America Online Inc -v- LCGM* (46 F Supp 2d 444); *America Online Inc -v- Prime Data Systems* (1998 US Dist LEXIS 20226) and *America Online Inc -v- IMS* (1998 US Dist LEXIS 20448): spamming amounted to "wilful infringement of [America Online Inc's] registered and service marks both by diluting the marks and by falsifying the origin of the email messages in violation of the Lanham Act". (Falsification of trade origin is a separate cause of action under the Lanham Act, co-existing with trade mark dilution.)

118 See for example: *Ebay Inc -v- Ebay4sex.com* (WIPO, D2000-1632); *Royal Bank of Canada -v- D3M Domain Sales* (AF-0147), and *Vert Tech -v- Computer Chronicles* (WIPO, D2000-1144).

119 See, for example, *Bally Total Fitness Holding Corporation -v- Faber* (29 F Supp 2d 1161).

120 Described at Section (C)2.1 above. See also *Lucent Technologies -v- Lucentsucks.com* (95 F Supp 2d 528): "a successful showing that lucentsucks.com is effective parody and/or a site for critical commentary would seriously undermine the requisite elements for the causes of action [under the ACPA]".

121 In *Quirk -v- Maccini* (FA00060009464) the Panellist considered the *Bally Total Fitness* case, but "respectfully disagreed" with the decision. Similarly, in *Diageo plc -v- Zuccarini* (WIPO, D2000-0996) the Panel took into account the position under US law, but declined to reach the same conclusion as the US courts for the reasons set out in the main text above.

122 *National Westminster Bank PLC -v- Purge IT* (WIPO, D2000-0636). See also *Direct Line Group Ltd -v- Purge IT* (WIPO, D2000-0583); *Dixons Group PLC -v- Purge IT* (WIPO, D2000-0584); and *Freeserve PLC -v- Purge IT* (WIPO, D2000-0585).

123 For criticism of these decisions see Solomon (footnote 75 above) and Mutimear (footnote 64 above) who describes the test adopted by the Panels as that of a "moron in a hurry". In *Wal-Mart Stores Inc -v- wallmartcanadasucks.com* (WIPO, D2000-1104) the Panellist commented: "distasteful conduct should not stampede UDRP decision makers into an unwarranted expansion of the domain name dispute process. The UDRP has a narrow scope. It is meant to protect against trademark infringement, not to provide a general remedy for all misconduct involving domain names ... bad faith, no matter how egregious, cannot supply a likelihood of confusion where it does not otherwise exist". He found that there was no confusing similarity between the complainant's marks and the impugned domain names and that criticism could also form the basis of a claim to a legitimate interest in a domain name.

124 Although the Second ICANN Staff Report (available on ICANN's website) describes the limitations of the UDRP as a "feature, not a failing".

## Useful Sites

| Organisation | Website address |
|---|---|
| **ICANN** | www.icann.org |
| General Information on the UDRP | www.icann.org/udrp/udrp.htm |
| UDRP | www.icann.org/udrp/udrp-policy-24oct99.htm |
| UDRP Rules | www.icann.org/udrp/udrp-rules-24oct99.htm |
| History of the UDRP | www.icann.org/udrp/udrp-schedule.htm |
| Statistical summary of UDRP proceedings | www.icann.org/udrp/proceedings-stat.htm |
| Searchable database of UDRP decisions | www.icann.org/udrp/udrpdec.htm |
| **WIPO** | www.wipo.org |
| WIPO Centre for Dispute Resolution | www.wipo.int |
| WIPO UDRP Supplemental Rules | www.wipo.int/domains/rules/supplemental.htm |
| **CPR Institute** | www.cpradr.org |
| **E-resolution Consortium** | www.eresolution.ca |
| **National Arbitration Forum** | www.arbforum.com |
| **Network Solutions Inc** | www.networksolutions.com |
| NSI Dispute Resolution Policy | www.domainmagistrate.com |
| **Nominet UK Limited** | www.nic.uk |
| Nominet UK Dispute Resolution Policy | www.nic.uk/ref/drs.html |