

INTERNATIONAL INTERNET DOMAIN NAME AND TRADE-MARK STRATEGY

by:

Jonathan C. Cohen
Senior Managing Partner
Director - ICANN

and:

Dr. Victoria Carrington
Partner

SHAPIRO, COHEN
112 Kent Street, Suite 2001
Ottawa, Canada
T: (613) 232-5300 F: (613) 563-9231
www.shapirocohen.com

July, 2002
NYIPLA
New York

INTERNATIONAL INTERNET DOMAIN NAME AND TRADE-MARK STRATEGY

Until fairly recently, more precisely, before the commercialization of the Internet, running even a small neighbourhood business involved a substantial investment of time, money and other resources. Anything on a scale larger than a small sole proprietorship would require compliance with numerous formalities, such as the requirements of local corporate statutes and regulations, and as the business grew beyond the borders of its initial geographic location, so too would its obligation to comply with the rules of any new jurisdiction(s) where it commenced operations, together with an increased exposure to liability in such jurisdictions.

Also until fairly recently, the concept of a comprehensive intellectual property management strategy which encompasses both the protection of one's intellectual property rights as well as the avoidance of liability was of interest mainly to corporate entities operating on a certain scale, usually at least regional, national or international in scope. Such entities would typically, over time, develop or acquire sufficient intellectual property, whether trade-marks, copyright, patents or industrial designs, to necessitate a structured approach to managing their portfolios in order to adequately safeguard and increase the value of these IP assets in their home country as well as any others in which they would operate. Even medium and smaller businesses have traditionally benefitted from the exercise of identifying their IP assets and determining the level of formal protection that could and should be obtained on the most cost-effective basis. But regardless of the size of the business, or the number of borders its activities crossed, or the formality of its IP management strategy, in the pre-Internet days it was a given that there was at least a clear set of national rules for each jurisdiction of interest, together with experts (network of associates) in each jurisdiction and extensive jurisprudential interpretation thereof which could be relied upon for guidance with some degree of certainty.

Everyone knows that the Internet has significantly and irrevocably changed this familiar business landscape. An enterprising individual with a great idea and a computer can now relatively easily, inexpensively and most importantly, virtually anonymously launch a successful international business and operate it from his or her desktop, targeting consumers in his or her home state or on the other side of the globe with equal ease.

Depending on how one looks at it, this not only has the positive effect of

liberating the legitimate entrepreneurial talents of a vast segment of the population whose dreams of running their own businesses were previously out of reach, it also fosters the epidemic of bad-faith actors who prey on the intellectual property of others and who can easily capitalize on the lack of a coherent, harmonized international regulatory framework for the Internet, a global communications medium that functions seamlessly but is nonetheless comprised of well over 250 independent national and general top level domain registries, only the latter of which are currently “directly” under the ICANN umbrella. This adds a whole new plane on which IP rights require protection (particularly trademark rights) and for those who choose to conduct business online, the accessibility of a web site on every computer that is connected to the Net anywhere in the world expands the risk of liability to include potentially every jurisdiction on the planet. In addition, domain names have been thrown squarely into the IP mix and should, as a rule, form part of an overall IP protection strategy rather than being considered merely as an afterthought or as just a hybrid trademark.

Accordingly, no longer do you have to be a large multinational with dozens of trade-marks registered around the world and an extensive Internet presence to consider implementing an international trade-mark / domain name strategy. Today, if you own a business of virtually any size and in any country, the question you must ask yourself is not **whether** you need an international trade-mark / domain name strategy, it is **what kind** of international trade-mark / domain name strategy do you need to effectively protect whatever IP assets you may have (even if it’s only a trade-name) and/or to prevent liability that is unexpected both in occurrence and jurisdiction. And if you are an intellectual property law practitioner, you must be prepared to answer this question for your clients based on an ever-expanding knowledge base. The concept of an IP strategy has thus entered the mainstream, with domain names often assuming a role of equal - and sometimes greater - significance than that of trade-marks.

When IP problems in the domain name system (DNS) initially began to surface, even companies that were accustomed to managing their trade-marks like any other assets were slow to recognize that failure to revise their IP management strategies to include domain names could become a very costly mistake. Accordingly, trade-mark / *domain name* strategies tended to be developed on an *ad hoc* or reactive basis - businesses would suddenly find their major marks appropriated by a cybersquatter (in .com, .net or .org, the TLDs of choice at the time) and in those early days, the only options open to cybersquatting victims would be negotiation or litigation, on a case by case basis.

There was also only one registry in those days, NSI, thus one could always find jurisdiction in the United States, and at least for American plaintiffs litigation in their home courts was a reasonable option. For non-Americans, registration in a ccTLD would therefore have probably made more sense. The courts (particularly in the U.S.) initially grappled with the challenges posed by trying to apply well-established and geographically circumscribed legal principles of jurisdiction, conflicts of laws and trade-mark laws to a medium whose nature defied such artificial delimitation, but eventually most issues were reasonably settled and the volume of cases was enough to develop a body of law that dealt effectively with cybersquatting, at least in the United States. Comparable jurisprudence quickly developed in various other highly industrialized nations with similarly open national TLDs. For a time therefore, a passing familiarity with the major cases and the awareness that business clients would often be better served by a more pro-active approach to domain name registration would suffice for the “domain name” part of trade-mark / domain name strategy advice.

As most of us are aware however, the events of the last two or three years have again dramatically changed the Internet landscape. Once the United States government turned over “Technical Management” and “Policy Oversight” responsibilities for the Internet to ICANN (Internet Corporation for Assigned Names and Numbers) a flurry of developments followed and continue to happen on an ongoing basis which have had a significant impact on both the domain name system (DNS) and our clients who seek to protect the integrity of their IP rights in the DNS. And in order to properly advise clients in devising an international trade-mark / domain name strategy, it is no longer sufficient to merely keep abreast of emerging caselaw - it is equally essential to have a fundamental awareness and understanding of these developments on an ongoing basis, for example:

- The gTLD Registrar function, which had been monopolized by VeriSign (f/k/a Network Solutions, or NSI) was opened up to competition and quickly became an international business in itself;
- The implementation of ICANN’s Uniform Domain Name Dispute Resolution Policy (UDRP) and its incorporation by reference into the service agreement for every single domain name registered in the gTLDs anywhere in the world meant that it was no longer necessary to engage in time-consuming and extremely costly litigation (at least in the first instance) in order to resolve the most obvious conflicts relating to abusive registrations of these types of domain names;

- The voluntary adoption of the UDRP by nearly 30 ccTLD administrators, and the implementation by at least 30 other ccTLDs of their own dispute policies (i.e. UDRP-type policy, or some form of mediation or arbitration) has given trade-mark owners additional options in a number of foreign jurisdictions;
- The introduction of new general TLDs by ICANN (.biz, .info, .name, .pro, .coop, .aero and .museum) provided significant and welcome alternatives to the .com namespace but raised concerns in the IP community that the problems plaguing the original TLDs would simply be perpetuated in these new TLDs ;
- The growing popularity of the roughly 250 ccTLDs on various fronts: among citizens of countries around the world who are increasingly turning to their national domains rather than one of the TLDs to establish an Internet presence; as well as among abusive registrants who have moved on from .com and are still able to carry on their bad-faith activities shielded by the inadequate rules of the many “cybersquatter” havens among ccTLD registries;
- The introduction of IDN - international or multilingual domain names;
- The amendment of the *Lanham Act* in the United States by the introduction of the *Anticybersquatting Consumer Protection Act*.

These are just a few of the major events that have taken place since ICANN was formed and the implications for trade-mark owners and domain name registrants is staggering. A sound trade-mark / domain name strategy that is ***international*** in scope has therefore become essential irrespective of the scale or geographic scope of the business, or the size of its trade-mark portfolio, if any.

The strategy itself may be anywhere on the spectrum from quite simple (i.e. the mere registration of a single existing trade-mark or trade-name as a domain name in one’s home ccTLD, or conversely seeking trade-mark protection for an existing domain name, if it is being used as a trade-mark) to complex (i.e. the registration of thousands of domain names across multiple TLDs corresponding to exact spellings and common misspellings of a company’s main marks, coupled with an aggressive policy of pursuing the registrants of any offending domain names), but its effectiveness can only be ensured by a careful

consideration of the many relevant factors on an **ongoing basis**. In other words, in order to **remain** effective, a trade-mark / domain name strategy should be kept current by means of a periodic review that takes into account not only the rapid and relentless pace of developments in the DNS around the world but any changes within the business itself that the strategy is designed to protect.

With respect to the primary focus of an effective international trade-mark / domain name strategy, the issue of cybersquatting *per se* has become somewhat less of a concern than it originally was, at least for larger businesses. This is because, as noted earlier, the jurisprudence of many countries has now successfully tackled the problem, but more significantly, the UDRP, which is mandatory in respect of all domain names registered in every gTLD as well as in some 30 ccTLDs (see list in Annex A), has proved to be a resounding success in providing a quick and comparatively inexpensive alternative to litigation for the clearest and most obvious cases of abusive domain name registration.

Nonetheless, for a small to medium-sized business, cybersquatting can still be a costly problem ¹, and for **all** businesses the UDRP cannot help if a conflict develops between legitimate competing third party interests on the Net.

The issues that people are increasingly wanting to cover in an international trade-mark / domain name strategy include questions about what kinds of proactive steps a business can take to *prevent* problems before they happen, for example:

- I do not currently do business online. Why should I care about the Internet?
- there are all these gTLDs, with more new ones on the way, as well as over 240 ccTLDs - where do I register? what do I register? my principal mark? everything that looks or sounds like it? One doesn't need to be a math whiz to immediately realize that unless your business is called Microsoft, registering even a handful of trade-marks as domain names across the board is not (for most) a viable option.

¹ Although it is significantly cheaper than bringing a court action, proceeding with a UDRP can also cost several thousand dollars depending upon the complexity of the case, which may still be difficult for many small businesses to handle. In addition, even though collectively the UDRP, the ACPA and current jurisprudence have been effective in significantly curtailing the cybersquatting problem in general, it has not been eliminated entirely - many cybersquatters simply do the math and make sure they demand a lower "ransom" than the cost of even a simple UDRP proceeding.

- if I register a domain name in a particular ccTLD, can I be sued in that country?
- if I discover that my trade-mark or trade-name has been taken by someone, do I have to sue or otherwise pursue them somehow? What options do I have? What if they are in another country? What if can't locate the registrant?
- now that I've created a domain name portfolio for my business, what else do I need to do?

Finding appropriate answers to questions like these, and the many others that should be asked when developing an international trade-mark / domain name strategy requires expertise in at least the following areas:

- trade-mark law in at least one country and a general awareness of trade-mark law and requirements on an international basis;
- domain name law in the home country and major developments in international jurisprudence and legislation (i.e. *ACPA* in the U.S. and its strong extraterritorial effects);
- an appreciation of the nature of Internet governance, the ICANN process and the ongoing developments therein listed earlier, the DNS and its main players, the contractual framework in place between the USG, ICANN, Registries, Registrars (or the lack thereof, in certain TLDs) and ultimately registrants and the effect this has on the situs of the domain name registration agreement;
- experience with ICANN's UDRP and at least an awareness of other dispute resolution alternatives, such as those that exist in numerous ccTLDs;
- general familiarity with the different types of TLDs: general v. country code, chartered v. non-chartered, open v. closed, and an awareness of the vast discrepancies between the rules governing the various TLDs around the world, how these differences could be used to the advantage of a client and to identify TLDs that could potentially be problematic. - i.e. the availability of an adequate WHOIS or lack thereof, relationship if any with ICANN, relationship with WIPO, availability of dispute policy such as the

UDRP or other form of formal or informal policy etc.

Putting the “domain name” in an international trade-mark / domain name strategy

The first step is recognizing that this is not a “one size fits all” concept.

As tempting as it may be, the best and most comprehensive strategy for a particular business, even for some of the world’s largest companies, may not be an all-out defensive and offensive campaign to register as many domain names (corresponding to as many permutations and misspellings as possible of every trade-mark they own) in as many TLDs as possible and to hunt down all interlopers without fail. As many companies have discovered to their chagrin, there can be certain pitfalls to this approach:

- “Domain Name Overload”: various analysts have researched the trade-mark / domain name strategies of some of the world’s top brands and note that on average, these businesses hold over 1000 domain names each ². However, although the registration strategies themselves may be sound, for some of these companies the effectiveness of the overall plan is compromised because:
 - (i) they are failing to utilize their domain names as constructively as possible, i.e. many domain names, including the deliberate misspellings of major marks that they have registered to thwart “typosquatters”, are simply being parked rather than pointed to the companies’ websites, and thus valuable Internet traffic and potential consumers are lost, possibly to competitors;
 - (ii) they fail to adequately consolidate their domain name portfolios, for example, after corporate mergers, or by having

² According to a survey of the domain name assets of the “world’s most valuable brands” by NetNames, a domain management company in the United Kingdom, companies such as Microsoft and The Walt Disney Company were at the top of the list, holding over 3000 domains each in their portfolios. Other large companies, such as Coca Cola, Nokia and Ford each hold between 200 and 1000 domains. (NetNames Press Release: *Top brands fall victim to domain name overload with 1000 names each* - February 14, 2002 at <<http://www.netnames.com/dnrs/netnames.client.Login>>; visited on July 19, 2002).

too many people responsible for domain name registration, or simply neglecting to ensure that contact details are kept up to date. This can result in important domain names going unregistered or unrenewed.

- “David & Goliath syndrome”: overzealous attempts by trade-mark owners to retrieve any and all domain names corresponding to their marks could easily cause unwelcome bad publicity, or worse, lead to claims of reverse domain name hijacking. Remember the case where Archie Comics, owner of the VERONICA trade-mark, went after the parents of 2-year old Veronica Sams, who had registered the domain name <veronica.org> to commemorate the birth of their little girl? Or the <pokey.com> case, where Prema Toy Co., owner of GUMBY and POKEY tried to divest a 12-year old boy (nicknamed “Pokey”) of the web site he got for his birthday from his father? Both cases settled, but not before the trade-mark owners were soundly ridiculed in the press. Canadian Tire fared little better when it chose to argue in a UDRP proceeding that <crappytire.com> was confusingly similar to its trade-mark and trade-name CANADIAN TIRE.

Clearly, a more balanced approach which systematically evaluates each aspect of the client’s business and tries to fit it into the “big picture” is usually more sensible and more cost-effective overall.

One should start off with a comprehensive analysis of what exactly the business is and what its objectives are - in other words, an inventory or profile of the business - with a view to answering at least the following questions:

- is it an established business or is it just starting out?
- is it local? regional? national? international? where is it domiciled?
- is the client “adventurous” in the domain name world (to be euphemistic)?
- what are its plans for expansion?
- what IP assets does the company have, or plan on acquiring, which may require protection on the Internet? trade-name? trade-mark(s)? domain name(s)? If it already has one or more domain names, how are they being used, if at all? what TLD are they registered with, what ISP etc. - e.g. where is jurisdiction capable of being found and over whom?,
- how important is the Internet to the business: does it currently have an Internet presence or is it planning to go online in the future?

- does it already have any domain name registrations, and if so, how are they being used, if at all?
- will it be posting an interactive website, conducting transactions online or merely using the Net to advertise its goods/services or provide information?
- what are the target regions/countries?
- does it really matter to the business operating in a single country if a web site marketing different goods pops up on the other side of the globe under the same domain name?
- who are the business's competitors? Do they have an aggressive Internet presence?
- has the business experienced problems with cybersquatting before? is this a business that is "likely" to do so in the future?
- what are the candidates for trade-mark and/or domain name registration: the trade-name? existing or proposed trade-marks? phrases or slogans?
- how much money is available to implement offensive or defensive measures? and which type of strategy is better?

Answers to these and other similar basic questions help determine the scope of the trade-mark / domain name strategy that most effectively balances the cost of implementation with the client's needs. Clearly, the same strategy will not be appropriate for both the "two trade-mark outfit in Hamburg" that is interested only in a limited German market and wishes to operate a modest informational web site for its domestic consumers, and the Coca Cola's of the world who can go to virtually any length to protect their vast and valuable trade-mark portfolios on the Internet.

Once a comprehensive inventory has been taken of the business, it is necessary to review the findings in light of the intricacies of the DNS as well as trade-mark law in order to marry trade-mark and domain name protection as effectively and as efficiently as possible for the client. In addition to the considerations customarily applied to planning a trade-mark portfolio, the following issues should also be looked at to determine (i) what domain names should be registered, and (ii) in which TLDs.

(i) Which domain names?

- as in the case of trade-marks, the very first step should generally involve searching. If a business is starting out with a domain name, it is essential to perform a comprehensive trade-mark search before adopting it to

prevent costly disputes later on. The reverse is equally important - a domain name search should routinely be included in every trade-mark search, even if an Internet presence is not immediately a high priority. It would be frustrating to invest significant resources into establishing a trade-mark or brand only to discover that it is not available for registration as a domain name in the TLDs of choice or, even worse that there is a domain name somewhere that has acquired trade-mark status and rights in one or more jurisdictions, but hasn't yet been registered anywhere as such (Like real estate, there are three important considerations here: liability! liability! liability!).

- in the case of numerous trade-marks, trade-names etc.:
 - are all the marks/names/slogans of equal importance, i.e. is it necessary to register them all as *both* trade-marks and domain names, or is one kind of registration more appropriate than the other in a given situation?
 - which is the best one to choose for the purposes of promoting the company's web site (bearing in mind that on the Internet, the domain name often automatically becomes the brand name)?
 - is there a core mark which is particularly vulnerable to cybersquatters / typosquatters? If so, it may be worthwhile to concentrate defensive registration efforts on it, including registering likely misspellings of a mark (remembering to actually use them to point to the main site, rather than simply leaving them inactive).
- is there a possibility that the business may be the target of "sucks", "anti-" or other criticism sites? Even if so, a "zero tolerance" policy may not be necessary unless it really is resulting in confusion or significant damage. It is usually preferable to evaluate on a case by case basis.
- does use of the domain name(s) in any of the countries of interest give the client enough rights in it to forego the expense of obtaining trade-mark registration in those countries?
- would it be advantageous to register certain domain names translated into

different languages or in one or more of the 39 different non-ASCII foreign language character sets that are available such as kanji, russian, hebrew (multilingual domain names, or IDN)?

- conversely, there may be certain English words that have very different meanings in other languages, therefore linguistically sound alternatives should be considered if appropriate.

(ii) Which TLDs?

Once an initial list of domain names that should be registered has been determined, the next fundamental question is which TLDs to register them in. The answer to this question could very well result in a significant modification of the list, if, for example, it appears that it would be more beneficial to register the primary mark as a domain name across a broader range of TLDs to take advantage of certain registries' rules (or prevent unscrupulous parties from doing so) than to register a large number of the mark's variants in a single namespace. Liability considerations will also affect the choice of TLDs. Accordingly, some of the key issues are the following:

- is the TLD open to all registrants (i.e. .com or .tv) or are there rules restricting (i) the purpose of domain name registrations according to the registry's charter (i.e. .biz) or (ii) the type of registrant according to domestic presence requirements (i.e. .ca is available only to entities that meet the Canadian presence requirements specified by the registry CIRA) or legal status (i.e. corporation v. individual)?
- does the TLD have a limit on the number of domain names that may be registered by a single entity?
- if the TLD has multiple second levels (i.e. .co.uk; .com.au) which are appropriate or available pursuant to the registry rules?
- does the TLD have an accessible online WHOIS service and how useful is it? This is one of the most important areas of inquiry when devising a strategy. Less than half of all ccTLDs (approximately 116 registries) have a WHOIS service (see list in Annex A), but not all of them provide full contact details for the registrant, including street address, phone, fax, e-mail and

DNS configuration. Some registries provide limited information such as registrant name only (i.e. .ws - Western Samoa) or charge a fee for the information. This issue is relevant primarily in the case of the ccTLDs which are not currently obligated to conform to the standards established by ICANN for all gTLDs. Such standards include providing access to adequate WHOIS records for all entries in the registry. Without access to proper, up-to-date WHOIS information it is practically impossible to locate the registrant of a domain name should it become necessary in the event of a dispute. While it may be possible to determine who provides connectivity to an offending web site by tracing the web site's IP address within the DNS and subsequently consulting the RIR WHOIS in an effort to shut the site down, this still falls short of identifying the registrant and is of limited assistance in any event if the domain name in question is inactive. A client could therefore choose to register domain names in ccTLDs without an adequate WHOIS service (if permitted by their rules) as a defensive measure to prevent third parties from doing so and remaining virtually untraceable, but it could also choose to do so if the relative anonymity offered by such ccTLDs would be of benefit to the client.

- does the TLD have a dispute resolution policy? As noted earlier, the UDRP is mandatory in respect of all domain names registered in the gTLDs, including the new ones. In contrast, just over 20% of ccTLDs have adopted an ADR procedure. At the time of writing, the UDRP (under the administration of WIPO) has been voluntarily adopted by at least 27 national registries, while at least 30 others have implemented their own dispute policies ranging from various forms of mediation or arbitration to policies modeled closely on the UDRP (see Annex A for lists). A client may accordingly choose to focus its often scant resources to taking defensive measures in TLDs where a convenient dispute policy is *not* available.

Liability issues

The issue of jurisdiction is just as important from the client's perspective when it is registering its own domain names as it is when trying to retrieve a domain name from a cybersquatter. What many people fail to realize is that the careless choice of *where* a domain name is registered can result in being sued in an unexpected, and possibly very undesirable jurisdiction.

Judicial remedies can generally be sought in the jurisdictions of the

registrant, the registry, or the registrar/reseller. In addition, it is important to consider that there is an extensive contractual framework between the DoC, ICANN, and all gTLD registrars and registries which sets out, and provides ICANN with the means to enforce, the standards and obligations governing the activities of the gTLD registrars and registries - and the situs of these contracts is the United States. While being subject to U.S. law is unlikely to be a problem (or avoidable) if you are American, foreign clients may be unpleasantly surprised to find themselves before an American court because they registered their domain name through an American registrar, or in a registry located in the U.S. The reverse is almost certainly true as well.

Internet jurisdiction caselaw, particularly in the U.S. is highly developed and a detailed discussion of it is well beyond the ambit of this paper, however, there are certain issues that are relevant to devising an effective international trade-mark / domain name strategy, including the following:

- registering a domain name in a ccTLD: even if the client chooses a ccTLD for purely defensive reasons without intending to conduct business or otherwise create significant contacts with a foreign country, registering a domain name in its national registry may be interpreted by its courts as an attempt to target the consumers in that country and could therefore play a role in the courts' decision to exercise personal jurisdiction over the client. When selecting a ccTLD, it would be useful to assess their risk of liability in the given country (as well as the prevailing local judicial attitudes towards exercise of jurisdiction) and to possibly consider undertaking reasonable good faith efforts to prevent or discourage access by local users to a site by means such as disclaimers, web site notices, software blocking mechanisms etc. ;
- if the reason for choosing a ccTLD is to avoid U.S. jurisdiction, be certain that neither the registrar nor the registry, or the manager thereof is located in the United States (i.e. the ccTLD manager for Iraq is in Texas; for .tv the administrative contact is in Canada while the technical contact is in Los Angeles)
- legislation with extra-territorial reach: one example of an effective anticybersquatting statute with considerable extra-territorial reach is the *Anticybersquatting and Consumer Protection Act (ACPA)* in the United States, which has been used frequently and successfully against bad-faith registrants by American trade-mark owners since its introduction in 1999.

Two important features of the *Act* are (i) the availability of substantial statutory damages (in amounts up to \$100,000 per domain name) in addition to the array of traditional trade-mark remedies for *in personam* actions and (ii) the provision of *in rem* jurisdiction, which is a powerful tool in situations where the defendant (registrant) cannot be identified or personal jurisdiction over the would-be defendant cannot be obtained by the trade-mark owner. The significance of this legislation to clients, particularly to non-U.S. domain name holders and U.S. entities whose rights are being infringed by non-U.S. domain name holders, has recently increased in light of the decision of the District Court for the Eastern District of Virginia in *CNN v. CNNews.com*³ (currently under appeal). In this case, the owners of the U.S. registered trade-mark CNN sued the domain name <cnnnews.com> which had been registered by a Chinese entity through a Chinese registrar. The registrant argued that it did not have sufficient minimum contacts with the U.S. to subject it to jurisdiction, given that it conducted its business exclusively in China through its Chinese language web site and had registered the name through a Chinese registrar. The Court in *CNN* held that *in rem* jurisdiction was proper under the ACPA because the domain name itself was located within the forum, by virtue of the presence of the .com registry (Verisign) in Virginia. This is the first case under the ACPA to hold *in rem* jurisdiction based on the location of the registry rather than the registrar, and thus appears to make every .com registration subject to U.S. in rem jurisdiction irrespective of the registrants contacts with the U.S. Clearly, for a non-U.S. business who intends to steer clear of American courts, registering in any TLD that has a U.S. registry or other significant U.S. connection may not be an attractive option.

³ 162 F. Supp. 2d 484, 2001 U.S. Dist. LEXIS 14693 (E.D. Va. 2001)

Of course often it is difficult to implement the optimal international trade-mark / domain name strategy for a client, at least initially, because advice is sought only when they have already taken certain steps, i.e. registered a number of domain names on their own in one or more TLDs and have encountered a problem either because of, or despite their efforts. This is a frequent occurrence given that domain names can generally be registered relatively easily and inexpensively. All too often, little, if any trade-mark or domain name searching has been done and virtually no thought has been given to jurisdiction issues. Yet these are all questions which should be asked right at the beginning, and as discussed at length, it is only possible to answer them competently if one has a fairly good understanding of key issues such as the gTLDs, the ccTLDs, ICANN, the relevant contractual relationships between them, the importance of adequate WHOIS services or dispute policies or the lack thereof, the significance of the location of a given registry or certain precautions that should be taken to minimize the risk of a foreign court exercising personal jurisdiction should the client have the misfortune of being sued there. Many of these issues also have technological and/or political components and a knowledge of these can further enhance the quality of advice.

I would conclude with some final thoughts and a hypothetical to illustrate some of the issues discussed herein.

First, when it comes to the world of domains, it is not necessary to be a lawyer to advise clients, register domain names and even represent a party in a UDRP proceeding. Both clients and advisers are also no longer tied to a particular jurisdiction in respect of many aspects of domain name/trade-mark portfolio management: for example, Canadian counsel can effectively advise a Japanese multinational and conduct UDRP proceedings on its behalf, calling in local advisers if necessary.

The second and final thought is, why you should care about ICANN and its Intellectual Property Constituency (IPC) and why it is important to be as involved in the process as possible. The answer is simply so that you can give your clients a voice in, and ensure their interests are represented adequately in the developments that continue to unfold in the DNS and which have a serious impact on intellectual property rights. The IPC has been an effective advocate to date for the international IP community, due in great part to the enthusiastic participation of the representatives of most major IP organizations of the world, many of whom have worked tirelessly since the beginning of the process to bring IP concerns to the attention of the other Internet stakeholders and ensure that

they are addressed in the policies and contracts that are implemented by ICANN. There is still plenty of room for individual participation however, either directly in the IPC or through the Internet/DNS committees of the IP organizations in which you are all members, and everyone is strongly encouraged to take part in whatever capacity they are able to.

Now for that hypothetical...

Your client comes to you in distress. He has found a website at a domain name which is identical to his U.S. trade-mark, selling cheap knock-offs of his product. The web site content is clearly directed to your client's own market, (the U.S.) though the domain name is in a foreign TLD - .by. You do some checking - the ccTLD is Belarus - it has no accessible WHOIS, so you have no idea who the guy is who is blatantly infringing your client's IP. The client wants the website taken down now!

What do you do?

There probably is no definitive answer (but I have included some suggestions at the end of this paper as to where to start), (although this is one of the kinds of questions I would use if there were an exam to qualify a "trade-mark / domain name law expert") but there is a cross-section of options to try which are not necessarily obvious from a legal standpoint (and which I will leave you to think about!). This underscores the fact that it is no longer sufficient simply to be trade-mark lawyer / expert, or to have done some UDRP, or even to be current on domain name case law around the world. Rather, trade-mark / domain name "law" is becoming a speciality of its own separate from mainstream IP, and it increasingly requires constantly **updated** technical, political and economic knowledge of the constantly changing landscape of DNS policy and technology (i.e. ICANN process) **in addition to** knowledge of gTLDs and ccTLDs around the world **in addition to** knowledge of trade-mark law, domain name law and the UDRP - the latter are just basic prerequisites. The chances of giving complete and appropriate advice are significantly lessened if one does not take steps to incorporate these other areas into one's knowledge base.

Some ideas to consider in respect of the hypothetical above:

- does the ccTLD have UDRP or other ADR Policy?

- does it have any r'ship with ICANN?
- contact ccTLD manager asking for contact info for registrant - quote RFC 1591 which provides that registration authorities should provide such info
- locate the operator of the website - trace the IP address of its nameserver in the DNS then check RIR WHOIS to determine who provides connectivity
 - do they have an acceptable use policy that is being violated - can they be contacted and persuaded to take the site down voluntarily?
- consider invoking judicial remedies in following jurisdictions:
 - website location,
 - ccTLD or ccTLD manager location (if different),
 - registrar/reseller location (if one exists)
- is there a mutual enforcement treaty?
- do any of these jurisdictions have a usable anticybersquatting statute?
- consider approaching the gov't associated with the ccTLD, possibly through WIPO
- consider action in the US to prevent importation of infringing products