THE MANAGEMENT OF DOMAIN NAMES AND METATAGS WITHIN A COMPANY

I. NEED FOR REGISTRATION OF A WEBSITE

A. CREATION OF A PERMANENT DOMAIN NAME TASKFORCE

1. Why and how?

When GlaxoWellcome emerged with SmithKline and became GlaxoSmithKline, the board made this information public without keeping in mind the domain name issue; they did not have any domain name officer. The day of this announcement, someone registered the corresponding domain name. Such a story is not exceptional: everyday, around the world, this kind of accidents – "business opportunities" as far as cyber squatters are concerned – happen.

Any big company should have a domain name officer. It is usually someone within the legal department or within the board. In any cases, it must be someone with an effective access to the management level where decisions are taken.

In multinational companies, the situation is more difficult because of the number of subsidiaries and branches, and because these usually have some freedom within their country (for marketing purposes for example). If, above this, the company makes business under a large number of trademarks (some of them being only local for a specific country), the creation of a real domain name taskforce is necessary.

While creating and managing the taskforce, the key words to remember are: centralization in cooperation.

1. Centralization means, in this case, that the deeper the taskforce is involved in business decision (even when such a decision is normally targeted to a specific country), the best it is. It is strongly recommended that the taskforce have a president or a secretary.

   The taskforce will keep accurate data concerning, notably: the number of active domain names with their status and date of renewal, the list of all "close" names related to a "main" one (see next chapter), the technical data for each domain name, etc. Centralization can go so far as to include all billing issues. Indeed, when possible, one should avoid sending renewal

notices and subsequent bills directly to the account department, which could be overwhelmed or late to settle invoices after a long delay. Bills (or at least a copy thereof) should ideally be sent to the task force to ensure permanent use of the domain name.

2. Association means, in this case, that the task force must combine a good *geographical* representation (someone from the headquarter, together with representatives of the subsidiaries) and a good *skills* representation (the CEO is not always the best person: it might be the operating officer, the customer-care department and/or the marketing department). More often, besides permanent members – Chief Legal Officer or the counsel for example – the composition of the task force can vary depending the issue).

2. Outsourcing issues

More and more service providers are currently specializing in domain name assets management and survey. These companies offer a registering procedure in nearly all ccTLDs (see hereafter) and in all public gTLDs (see hereafter). They keep a single point of contact. Some of them provide monitoring for registrant's domain names and for competitors ones, as well as cyber squatting monitoring (in addition, they usually provide their customers with a software-based solution enabling online access to all available information).

B. CHOOSING A DOMAIN NAME

When choosing a domain name, the registrant must keep in mind at least two important things:

- Once the "main" domain name has been chosen, the registrant must analyze if "close" names should also be registered;
- Although it is often useful to register close names, it must be clear in everybody's mind that a zero-risk situation doesn't exists.

The list of close names must be made, bearing in mind all forms of cybersquatting, which includes notably:

- Cybersquatting (also called domain name grabbing): registering a domain name in order to sell it back later to the person – usually a company or a well-known person – whom, intuitively, should be the normal holder;
- Reverse domain name hijacking: people register a trademark that is identical to an existing domain name. Subsequently this person sues the domain name holder arguing that this holder violates his rights. This cybersquatting methodology is happily unsuccessful most of the time;
- Pointsquatting: a specific form of cybersquatting using the same address as the victim without a point after the famous "www" (for example http://www.company.com instead of http://www.company.com).
- [redacted] type-squatting: a specific form of cybersquatting using spelling errors (for example http://www.company.com instead of http://www.company.com).

For example, if the registrant wants to register <world of pleasure> as a "main" domain name, it might consider that the following are "close" names:

- world-of-pleasure
- world-of-pleasures
- a world of pleasure
- a-world-of-pleasure
- worldpleasure
- world-pleasure

This is a difficult and fastidious job, but it is actually the easiest way to avoid losing time and money in trials or other resolution procedures. Specific software can help the registrant to build the list.

The company might consider that the registration of some domain names is be compulsory. Usually this list includes at least all registered trademarks and any others sign on which the company has an exclusive right (for example, a commercial denomination or the name of the company, etc.).

While determining the main domain name and its close ones, the registrant must combine the *protection point of view* and the *target point of view* (see next chapter).

C. CHOOSING MEANTAGS

Metatags are HTML codes usually invisibles for the visitor, except if this one request to read the source-code of the webpage. There are various types of metatags[1] but the most famous one is designed to help search engines indexing and ranking websites according to their content. For example, a website concerning football will include at least the word "football" in its metatag.

A big difference between metatags and domain names is the absence of any kind of registration: any website holder can freely decide which metatags it wants to include in its source-code.

This modus operandi is frequently used in order:

- To raise artificially the number of visitors (putting "sex" in the metatags, even if the website has nothing to do with sex, in order to appear in the result-list each time someone types "sex" in a search engine);
- To grab some visitors (putting the name of a competitor in order to appear in the result-list each time someone types the name of the competitor in a search engine).

Besides these potentially illegal uses of metatags there are very useful utilizations:

- It is used by sponsors to be sure that they will appear in the result list each type someone try to get information concerning an event (for example, World-Cup sponsors are entitled to include "World-Cup" in their metatags);
- It can be used by a company to cross-reference its websites (for example, if the same product is sold in the world under different names and if there is one website per name, it might be useful to include in all websites all different names of this product).
- It can be used by group of companies or holdings to cross-reference all companies' websites;

The domain name taskforce will work in close cooperation with all departments of the company in order to make the list of all useful metatags. For example, the marketing department will provide the list of all events in which the company in involved as a sponsor, and the taskforce will make sure with the legal department that the contract with event's organization specify that the company's name or its product's name will be included in the metatags of the event's website.

[1] Including for example "revisit-after", "description", "keywords", "robots", "rating", "copyright", "author", "language", "generator", etc.

D. OPENING OF A gTLD AND OF A ccTLD

Once the various names have been chosen, the registrant must consider the Top Level in which it will apply for registration. Actually, there are two families of Top Level:

- The generic Top Level (gTLD), including the famous .com, .net and .biz. gTLDs are registered on a worldwide basis;
- The country code Top Level (ccTLD), registered on a national basis (.be, .fr, .us, etc.).

Some situations are quite simple. For example, all registered trademarks must at least be registered as a domain name in all countries (ccTLD) in which the trademark is registered. Other example: the company-site of a multinational company must at least be registered in all countries (ccTLD) in which the company is established. More often, the situation is more difficult to assess; because of this, some companies have decided, as a rule, that each time a domain name is registered, it is registered in all ccTLDs and gTLDs in which it is available (Coca-Cola, the "world company", works under this rule).

Taking back the example of www.worldofpleasure.com, if this is a site dedicated to a product sold solely in Germany, the taskforce might consider that it is worth registering it in .com, but also in .de and even in ccTLDs of Germany's neighbor-countries (Austria, Poland, Netherlands, etc.) because some customers might buy the product in Germany but originate from these countries.

While working on this issue, the registrant must in fact combine two different approaches:

1. The *protection point of view* implies that the registrant must protect its assets. For example, the registrant might decide that all intellectual property assets must be protected as a domain name in all countries and all gTLDs.

   In application of this point of view, when a registrant decides for a gTLD (.com for example), it will usually try to register in all other public gTLDs (.net, .biz, etc.). Consequences are easy to understand. Failing to comply with this principle, the White House registered only http://www.whitehouse.gov for its official website; very quickly, two other persons registered http://www.whitehouse.org (satiric site) and http://[redacted] (sex site)!

2. The *target point of view* implies that the registrant must, firstly, analyze the target of its website and, secondly, consider as compulsory to register at least all relevant TLDs taking into account this target. For example, if a product is

sold in different countries under different names, all national names must at least be registered in the corresponding ccTLD.

E. VERIFICATION PRIOR TO REGISTRATION

Once the names to register and their relevant ccTLDs and/or gTLDs have been chosen, the registrant should make a prior verification in the Whois? database, in order to be sure that there are no anteriority problems. Indeed, it might appear at that stage that a name, or a Top Level, has been pre-registered by somebody else.

It is important to underline that this verification doesn't mean that the name will be accepted when the registrant will apply; indeed, in most ccTLDs, there are strict rules to follow and the registration authority might refuse an application in respect thereof. Nor does it mean that the use of the name will be possible (for example, despite the fact that a name is granted to the registrant, a third-party might object to the use thereof, because of its intellectual property rights.

This verification is only meant to detect pre-registration of any identical domain name(s). It is nevertheless useful, notably for three reasons:

1. At that stage, it is usually still possible for the registrant to amend its plan, drop this name, or take action in order to get this name.

2. Searching the whois? database is anonymous, quick and easy. If a problem is discovered at that stage, it can thus be limited within the registrant's company. Failing to comply with this prior verification, company's secrets are sometimes made public involuntarily at the occasion of an aborted registration.

3. Registration problems, or aborted registration, is always a bad publicity for the registrant and can be an opportunity for its competitors.

[redacted]

- A company must consider its domain name assets at a **global and high level**;
- An effective domain name policy is part of the whole business plan of the company, and must rely on an extensive knowledge of company's activities, projects, trademark portfolio, etc.;
- It implies the participation of several persons in **close coordination**;
- When several domain names must be managed, it should mean a high degree of **centralization in cooperation** with concerned persons, subsidiaries or branches;
- The policy must be **flexible and progressive**.

II. REGISTRATION ON A WEBSITE

A. INFORMATION TO BE PROVIDED

1. Which information?

A great number of information must be transmitted to the registration authority, here are some of them, together with recommendations:

Registrant[2]	Registering a domain name in the name of a provider, or a company employee, or even under the CEO's name should be avoided or modified
Administrative contact[3]	The administrative contact plays a key role. It keeps permanently the operational power on the domain name and must be entitled to take domain name related decisions on its own. Therefore it is essential to give this role to a qualified person involved in the domain name management
Billing contact[4]	This contact will manage the renewals of the domain names on behalf of the company. It is important to underline that a great number of accident arise because of a bad billing contact (for example, the e-mail address of an employee that doesn't work anymore: the renewal notice is sent on this address and nobody take care of it)

[2] Please note that the exact wording can vary depending the country and/or the provider
[3] idem.
[4] idem.

Technical contact[5]	Ideally, this contact should be allocated to the ISP who has the responsibility of administering domain name servers on which are hosted domain names. In the case the company holds and manage itself its servers, the person in charge of them is usually the technical contact

2. How to provide this information?

Information provided must be constant and everlasting, independently from the physical person and from the provider; this is a key issue.

Indeed, if the information relies on a person or a provider, it must be updated in case of changing (an employee going to another company or to another department within the company, or changing of a provider). In reality, it is a fact that updating is rarely done, with, sometimes, tremendous consequences including the deletion of the domain name.

Email address	the email address should be a generic one (dns.admin@company.com) rather than nominal (bobmoore@company.com) in order to avoid [illegible] possible employee changes [illegible] to be paid to the continuity of the running of the email address. Another advantage of generic alias is to give the possibility to forward the mail received on this address to multiple persons within the company and even outside (lawyer or provider for example)
Postal address	the head office of the company is a guarantee as far as stability is concerned; however a lot of companies find it preferable to use the address where the contact person is located (administrative, billing, technical)
Phone number	As for the email and postal addresses, one must provide for the updating of phone numbers in case of relocation or move.

[5] idem.

B. THE ALLOCATION OF A DOMAIN NAME

In most of the gTLDs (.com, .net and .org notably), the registration is based on the principle "first come, first serve": there is no control by the registration authority at the moment of registration. The registration is automatically accepted if this name is available. By exception, some gTLDs are limited to certain applicants (.museum and .aero for example).

Some national ccTLDs work on the same "first come, first serve" principle (Belgium for example), but most of them have a strict registration policy in order to assess, prior to registration, that the registrant has a right to apply for the domain name.

Irregardless the existence of a prior control, a third-party can always request the registrant to stop using this domain name and/or transfer it to him. In most of the cases, such an action is based on intellectual property issues, fair practices and competition rules (see hereafter: enforcement).

C. THE METATAGS

A big difference between metatags and domain names is the absence of any kind of registration: any website holder can freely decide which metatags it wants to include in its source-code.

Needless to say, if the use of a metatags is an infringement to a law or a third-party's right, the domain name might face litigation (see hereafter: enforcement).

[illegible]

- It is important **to prepare** the information to be given at the moment of registration;
- This information must be **logical**, taking into account the situation of the company; it must be **independent** from a physical person and everlasting;
- Technical and billing informations should be **as harmonized as possible** within the group;
- Even if there is a prior verification by the registrational authority, the allocation of a domain name does not guarantee the company against a **third-party**;
- **Metatags** are free (provided, of course, that they do not infringe any law or any third-party's right).

III. USING A DOMAIN NAME

The most natural way to use a domain name is to put at that address a website, but it is not the only way to use it. One could notably imagine:

- To register a domain name without using it ("defensive registration"): it is often the case when a cyber squatter registers a domain name corresponding to a trademark in order to resell it later on, but it can also be used when the marketing or the R&D department is close to initiate a new product or campaign and wants to be sure to get the best name;
- To register a "waiting page": the site contains no information except a waiting announcement ("under construction" for example). Cyber squatters wishing to hide a defensive registration frequently use this modus operandi;
- To redirect the visitor to another website: this is typically the situation for "close" domain names.

IV. ENFORCEMENT ISSUES

A. MONITORING

As soon as a company considers its domain name asset as an important one, it must consider the monitoring thereof.

This task is usually outsourced to a specialized provider using sophisticated monitoring services, scanning the web and registrations (some of them on a worldwide basis including ccTLDs) to detect all potentially harmful uses. The list of "close" names made prior to the registration is often of a great help, but new software use a lot of other technical tools, including the monitoring of metatags (see hereafter).

It must be stressed that it makes no sense to organize a monitoring on domain names if the same procedure is not applied to metatags. In reality, metatags are potentially more harmful because they are difficult to detect and monitor.

B. ENFORCING

Once a company decided to fight a harmful use, three attitudes are possible: out-of-court settlement, ADR or legal proceeding.

1. Out-of-court settlement

Needless to say, the parties can settle out-of-court agreement. Despite the fact that the price is frequently high, it is very often less than the cost of a judiciary procedure and is quicker.

2. Alternative Dispute Resolution (ADR)

ADR is a dispute resolution process in which the parties agree to submit their problem to an arbitration panel.

The UDRP (Uniform Domain Name Dispute-Resolution Policy) is one of the most famous ADR process, focused on gTLD domain names conflicts. It has been drafted in collaboration between the ICANN[6] and WIPO[7]. Each gTLD registrar must insert a clause in its contracts making the UDRP mandatory for gTLD owners.

The complainant in a UDRP process must demonstrate three elements:

- The domain name is identical or confusingly similar to a trademark or a [redacted] in which the complainant has rights;

[6] Internet Corporation for Assigned Names and Numbers. ICANN is the non-profit corporation that was formed to assume responsibility for the IP address space allocation, protocol parameter assignment, domain name system management, and root server system management functions previously performed under U.S. Government contract by IANA and other entities. ICANN delegates also the power to national registrars to alloy IP address and related national domain names.

[7] World Intellectual Property Organization; http://www.wipo.org.

— The registrant has no rights or legitimate interests in respect of the domain name in question;

— The domain name has been registered and/or it is being used in bad faith. Assessing the bad faith, the arbitration panel will take into account all available element, notably:

  - Circumstances indicating that the Domain Name was registered or acquired primarily for the purpose of selling, renting or transferring it to the Plaintiff (complainant);

  - The domain name was registered in order to prevent the owner from reflecting the mark, provided that the registrant has engaged in a pattern of such conduct;

  - The domain name was registered primarily for the purpose of disrupting the business of a competitor;

  - The domain name was registered with the intention to gain Internet users by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation or endorsement of the registrant's site or of a product or service. It must be underlined that the possibility of confusion, especially for the consumer is the central criterion.

Despite this *uniform* dispute resolution process, it is well known that some arbitration panel (WIPO for example) is more in favor of trademark holder than others. Depending the nature of the underlying right of the complainant, it might be useful to make an "arbitration forum shopping".

Two of the main advantages of UDRP include the fact that:

— It ensures effectiveness of the decision: if the panel finds in favor of the complainant and grants a transfer of the domain name, the transfer will be automatic if the defendant does not bring a legal proceeding before a judicial court within a fixed delay;

— If it impossible to locate the cybersquatter (for example because he gave a false address at the moment of registration), it is sufficient to prove to the panelist that all reasonable efforts have been done and that the domain name owner remains unreachable.

The cost of UDRP arbitration vary between U$ 1.500 and U$ 2.000 for a conflict involving 1 to 10 domain names and requiring one panelist (judge/arbiter). There is no system for reimbursing the attorney fees.

UDRP is also available for certain ccTLDs (when the national authority adopted it[8]). Despite the fact that UDRP is not applicable in other countries for ccTLD disputes, similar principles usually apply.

3. Legal proceedings

A plaintiff is of course entitled to seize a judicial court.

It is frequently a long-run process, notably because of international aspects. Plaintiff must first determine in which country it will bring the procedure and which law the judge will apply. Furthermore, even if the court finds in favor of the complainant, its ruling might not be applied if the holder is located in another country.

This said, legal proceeding could be more advantageous in some circumstances, for example when plaintiff and defendant originate from the same country, or when the legal ground of the action is competition-related more than intellectual property-related (experiment shows that arbitration panels are less friendly with competition and fair practices laws than with intellectual property one – in UDRP, the situation is still clearer since the panel is only competent if the domain name is identical or confusingly similar to a trademark or a service mark on which the complainant has rights).

If the complainant wants to get money from its action, it must generally go for a legal proceeding.

Etienne Wéry,
Attorney (Brussels and Paris bars)

Brussels, janv. 31, 2006

[8] .AC (Ascension Island), .AG (Antigua & Barbuda), .AS (American Samoa), .BS (Bahamas), .BZ (Belize), .PA (Panama), .PH (Philippines), .PN (Pitcairn Island), .CY (Cyprus), .EC (Ecuador), .FJ (Fiji), .GT (Guatemala), .LA (Lao People's Democratic Republic), .MX (Mexico), .NA (Namibia), .NU (Niue), .RO (Romania), .SH (St. Helena), .TT (Trinidad and Tobago), .TV (Tuvalu), .VE (Venezuela), .WS (Western Samoa).