Minimizing HARM

Proposal to reduce the need for defensive registrations in new gTLDs

Prepared by Melbourne IT as a Community Discussion Paper
15 August 2012 – Version 1

Executive Summary

ICANN has established a set of protections intended to protect the general public from being deceived or misled by unscrupulous persons or organizations using well-known distinctive names, or marks, without the right to do so, or in an otherwise inappropriate manner.

This paper makes the case that, despite the current protections ICANN has put in place, there is still a set of High At-Risk Marks (HARM) that remain particularly attractive to unscrupulous persons and organizations who will attempt to register these marks at the second level of new gTLDs.

The paper proposes a set of criteria for identifying marks that should be considered High At-Risk Marks, and proposes the following additional protections for High At-Risk Marks:

- The ability to pay for a Once-off Reservation Fee (ORF) during the sunrise process
- The requirement of new gTLD registries to validate at least two elements of a registrant's contact details: phone number, email address, or postal address
- The extension of the Trademark Claims process indefinitely
- Rapid take down within 48 hours of a Uniform Rapid Suspension (URS) complaint, unless a Response Fee is paid equivalent to the URS fee paid by the complainant (with the winner of the dispute receiving a refund on their fee).

1. Introduction

Distinctive names, or *marks*, help the general public to identify and differentiate products and services provided by organizations. These organizations may be in the public sector or private sector, and may operate for-profit or as non-profits. As a mark becomes well-known as a symbol of quality, trust, or service, unscrupulous people or organizations may take advantage of this reputation to mislead the general public. Misleading the public could be in the form of using a mark to label an inferior product or service, or using a mark to trick a member of the public to provide the unscrupulous person or organization with information, services, or money. Over time, a legal framework has been established, in both the international and domestic legal arena, to protect the general public from such conduct. International treaties protect specific names like Red Cross and Red Crescent, and set the foundations and groundwork for domestic trademark law. Individual countries implement national laws that are consistent with these international treaties.

The Internet domain name system (DNS) consists of over 200 generic top level domain names (gTLDs), such as .com, .net, .org, .biz, .info, and country code top level domains (ccTLDs), such as .uk (United Kingdom), .ca (Canada), .br (Brazil), .cn (China), and .za (South Africa). The system for registering domain names allows an organization to easily obtain, at low cost, an identifier that is globally unique based on their mark. Organizations typically register their organization's name, or the word mark of their products or services, at the second level (e.g. example.com) or at the third level (e.g. example.co.uk) of the domain name system. An organization with a global presence will often have a primary domain name in a gTLD like .com or .org, and a set of secondary domain names in the key countries in which they operate like .uk or .cn.

Unfortunately the domain name system does not prevent unscrupulous people or organizations to obtain a domain name that closely resembles an organization's name, or the mark of their products or services, in a TLD that is not being used by the organization. This domain name can then be used to mislead the general public. For example, if an organization has a primary domain name in .com, an unscrupulous person or organization may register an equivalent name in .net, .org, or .co for the purposes of misleading the public. This has led to a practice of *defensive registrations* being widely adopted, where organizations register their names and marks in many of the gTLDs and ccTLDs with open registration rules. An organization may have 20 domain names which they actively use in advertising, and in communications with Internet users, but may have 200 defensive registrations (which are not actively in use) to ensure that the public is not misled and that the mark remains protected.

Trademark laws in many countries have allowed organizations to take legal action in cases where an unscrupulous person has registered a domain name that uses a name that is a registered trademark for the purpose of misleading the public. However, the legal costs to do so can be substantial, and it has usually been cheaper and simpler to pay for a defensive registration. ICANN established a dispute resolution procedure called *Uniform Domain Name Dispute Resolution Policy (UDRP)* (http://www.icann.org/en/help/dndr/udrp/policy) , which has allowed many trademark owners to obtain a transfer of the domain name from the offending registrant. This is much cheaper than taking unscrupulous registrants to court, but is still more expensive than a defensive registration.

On 13 June 2012, ICANN announced that there were 1,930 applications for new generic top level domain names (new gTLDs). Many of these top level names are for categories like .hotel, .restaurant, and .sport, similar to phone directory categories, and others are for more generic terms like .store, .web, and .blog.

ICANN has established a detailed set of new protections for the consumer as part of the new gTLD program.

The new gTLD program will establish a Trademark Clearinghouse (http://newgtlds.icann.org/en/applicants/agb/trademark-clearinghouse-04jun12-en.pdf) for organizations to list the names or marks for which they have legal protection. New gTLD operators must implement a sunrise period where trademark holders will get the first right to register domain names in a gTLD, for either active use by that trademark holder, or as a defensive registration for that trademark holder. For 60 days after the sunrise phase, new gTLD operators must implement a Trademark Claims process, which will advise registrants of any trademarks that may exist on a name that the registrant is intending to register, and will advise trademark holders if a registrant registers a domain name at the second level that uses an exact match of their trademark.

ICANN has also implemented a process that a trademark owner can use to suspend a domain name that is being used to mislead the public called Uniform Rapid Suspension (URS) (http://newgtlds.icann.org/en/applicants/agb/urs-04jun12-en.pdf). A registrant subject to a URS complaint from a trademark owner has up to 14 days to file a response (with the ability to request up to an additional seven day extension). If the URS provider finds in favor of the trademark holder, the domain name will be suspended, but not transferred to the trademark owner. A trademark owner must pay a fee (intended to be around US$300, but may end up being higher) to have their claim investigated. A registrant pays no fee, unless more than 15 names held by the registrant are subject to a claim.

The framework established by ICANN provides sufficient protection for the vast majority of organizations that are trademark holders. Trademark holders will have the first right to register names in relevant categories (e.g. the Hilton hotel chain would have the first right to register in Hilton.hotel), and for categories that are not relevant, trademark holders will be able to rely on the URS and UDRP procedures to stop the misuse of names.

However, there is a subset of organizations that have *High At-Risk Marks (HARM)* that are repeatedly the target of unscrupulous persons or organizations that use online techniques to mislead the general public. This is particularly the case where consumers may be misled to either conduct online financial transactions, or provide highly confidential personal or financial information. Examples of such organizations that have high at-risk marks include PayPal and Red Cross. Unscrupulous persons or organizations use deceptive domain names to either obtain banking information, or financial donations in the case of the Red Cross. The new protections introduced by ICANN are not sufficient to avoid the need for organizations with High At-Risk Marks to pay for defensive registrations for most of the new gTLDs. If we assume an organization will need a defensive registration in 1,000 new gTLDs, at an average cost of $100 per year, this would equate to a cost of $100,000 per mark per year. This is because there is a high probability that unscrupulous persons or organizations will register their marks in many of the new gTLDs. This means that such organizations are likely to have to use URS to suspend the domain names, and the cost of URS will generally be higher than the cost of a defensive registration. There is no cost to an unscrupulous person or organization to respond to a URS, and the 21 day period before suspension is often sufficient for an unscrupulous party to get a financial return (e.g. from pay-per-click advertising or phishing attacks) from the typically low cost of domain name registration.

This discussion paper proposes some additional levels of protection for High At-Risk Marks based on the existing framework of protections being introduced by ICANN. It is expected that only a few thousand marks globally would fall into the category of High At-Risk Marks.

2. High At-Risk Marks (HARM)

It is proposed that, in addition to the protection mechanisms adopted by ICANN, the Trademark Clearinghouse provider allow trademark holders of High At-Risk Marks (HARM) to request that these marks be identified specifically in the Clearinghouse as High At-Risk Marks (HARM). There would be an additional fee, based on cost recovery for the provider, for validation of a HARM that would likely be in the region of ($1,000-$2,000).

A set of objective criteria should be used to identify a High At-Risk Mark, with two requirements to be met – a minimum number of the objective criteria need to be satisfied, as well as attainment of a minimum score against those criteria.

The proposed minimum criteria are:

- Legal protection (via trademark laws or other legal protection of the name) in at least three of the five ICANN regions (North America, Europe, Africa, Asia/Australasia/Pacific, Latin America/Caribbean). All trademark registrations must have been issued five years before the date of validation into the clearinghouse.
- The second level domain name for the organization's primary online presence must match the High At-Risk Mark (e.g. if the mark is "example", then a corresponding domain name would be example.com).
- The High At-Risk Mark must be distinctive and must not match common words (e.g. in dictionaries of 10,000 common words) used in the six UN languages (English, Arabic, Chinese, Spanish, Russian, French). (For example, marks like Apple or Gap may not be eligible)
- The organization should demonstrate that the High At-Risk Mark has been the subject to misleading and deceptive conduct online as evidenced by a minimum of five successful UDRP actions, court actions, or documented suspensions by a top ten registrar (which will have formal processes for determining when to suspend a domain name).

In addition to meeting the minimum criteria above, the High At-Risk Mark will need to obtain a minimum total points score of 100, where one point is awarded for each legal protection in a jurisdiction, and one point is awarded for each successful UDRP, court action, or domain registrar suspension undertaken in relation to the mark.

3. Sunrise Period

During the sunrise period of a new gTLD, it is proposed that in addition to a first right to register a High At-Risk Mark in a new gTLD as an active domain name registration, that an organization with a High At-Risk Mark have the right to pay a *Once-off Reservation Fee (ORF).* A domain name subject to a ORF will not be available for use by the organization, and a new gTLD operator may choose to have a webpage similar to that used for .xxx where the consumer is advised that the name is reserved from use (e.g. http://www.ibm.xxx). An ORF should be the same cost or lower than the cost of a registration during the sunrise period.

The benefit of a ORF is that an organization that does not wish to use a particular second level domain name, but wants to defensively register the name as there is a high likelihood that an unscrupulous person or organization may try to register the name, can pay a once –off fee rather than an annual registration fee to reserve the name to protect the public. e.g. If Red Cross does not want to use redcross.charity, there would be a high likelihood that another party may register that domain name. Red Cross should be able to pay a ORF fee to permanently reserve redcross.charity from registration.

4. Validation of registrant contact details

Many unscrupulous persons or organizations that set out to register domain names for these purposes utilize false contact information in the process.

Currently, the onus remains on registrants to ensure they provide valid and accurate contact details for the registrant of the domain name. Registrars are not required to validate the information submitted by registrants, unless it is advised that the information is believed to be false. In that instance, a registrar is required to investigate claims that the information is false and give the registrant time to correct it. This provides benefits to the vast majority of registrants that register domain names for legitimate purposes, as the costs of registration are kept low.

It is proposed that for High At-Risk Marks, gTLD registries be required to validate at least two of the following contact elements: phone number, email address, or postal address submitted by registrars on behalf of registrants. This may result in higher registration costs for these names – due to the extra costs incurred for validation, but this will only be for a small subset of domain names. While registrars could perform the validation, centralizing the validation at the registry will ensure a uniform high standard of data validation, and also provide a second level of validation beyond that which a registrar may use at time of registration. This validation should occur before a new domain name is live in the DNS. It would be similar to processes used by digital certificate authorities that often perform their own validation after a registrar submits information to the certificate authority, to ensure the integrity of the process.

5. Trademark Claims service

The current Trademark Claims service applies during the first 60 days of operation of a new gTLD after completion of the sunrise period. It requires a new gTLD registry to advise registrants of any trademarks that may exist in relation to a name that the registrant is intending to register, and will advise trademark holders if a registrant registers a domain name at the second level that uses an exact match of their trademark.

It is proposed that for High At-Risk Marks the Trademark Claims process should continue indefinitely. A new gTLD registry could store at the registry a list of the High At-Risk Marks stored in the Trademark Clearinghouse, which could be updated at regular intervals (e.g. monthly). This would avoid reliability issues with being dependent on the availability of the Clearinghouse at the time of registration.

6. Uniform Rapid Suspension (URS)

A registrant subject to a Uniform Rapid Suspension (URS) complaint from a trademark owner has up to 14 days to file a response (with the ability to request up to an additional seven day extension). If the URS providers finds in favor of the trademark holder the domain name will be suspended, but not transferred to the trademark owner. A trademark owner must pay a fee (intended to be around US$300 but may end up being higher) to have their claim investigated. A registrant pays no fee, unless more than 15 names held by the registrant are subject to a claim.

It is proposed that for High At-Risk Marks, that a domain name be suspended within 48 hours of the complaint, unless the registrant pays a Response Fee equivalent to the URS fee paid by the complainant. Once the registrant pays a Response Fee the domain name will be released from suspension, and the Registrant has up to 14 days to file a response, with the possibility of a seven day extension. If the complainant wins the dispute the name would be suspended under the existing rules of the URS. The winner of the URS dispute process would receive a refund of the fees that they have paid. This balances the cost of a URS proceeding between the registrant and the complainant.

If the registrant chooses not to pay the Response fee, or not to respond to the complaint at all, then the name will be suspended after 48 hours, and the URS provider will review the facts submitted by the complainant to decide whether the name should remain suspended. This provides a true “rapid” suspension process.

7. Conclusion

ICANN has introduced a detailed set of protections to minimize the use of second level domain name registrations to deceive or mislead the general public as part of the new gTLD program. For most trademark holders the framework established by ICANN should provide sufficient protection to avoid the need for defensive registrations at the second level of new gTLDs.

However, there is a set of High At-Risk Marks that are particularly attractive to unscrupulous persons and organizations whose attempt to register corresponding second level domain names in new gTLDs may be successful, despite the current protections.

This discussion paper proposes a set of criteria for identifying marks that should be considered High At-Risk Marks, and proposes the following additional protections for these marks:

- The ability to pay for a Once-off Reservation Fee (ORF) during the sunrise process
- The requirement of new gTLD registries to validate at least two elements of a registrant's contact details: phone number, email address, or postal address
- The extension of the Trademark Claims process indefinitely
- Rapid take down within 48 hours of a URS complaint, unless a response fee is paid equivalent to the URS fee paid by the complainant (with the winner of the dispute receiving a refund on their fee)

8. Acknowledgements

Melbourne IT would like to acknowledge the following parties that have developed components of the solution that are incorporated into this discussion paper:

- The Implementation Recommendation Team (IRT) report into Trademark Protection for new gTLDs (http://www.icann.org/en/topics/new-gtlds/irt-final-report-trademark-protection-29may09-en.pdf), which included the concepts of the Trademark Clearinghouse and the URS, as well as the idea of a Globally Protected Marks List
- The ICM Registry Launch Plan (http://www.icmregistry.com/launch/plan) which included the idea of once-off reservations (e.g. http://www.ibm.xxx)
- The Deloitte 100 brand list (http://www.deloitte.com/be/brand-list), which included a list of brands that make significant efforts to protect and enforce their trademarks in the domain name space, for use in the .co (Columbia) launch process.