

TLD Rights Protection Mechanisms

Potential trademark Rights Protection Mechanisms (RPM) at the 2nd level can be divided into three main areas – each defined by their time relative to TLD launch. These areas are:

- 1) Pre-Launch
- 2) At-Launch
- 3) After-Launch

Of these, we believe the third, “After Launch,” is the most fruitful path to explore. We believe it offers the most potential to protect the rights of trademark holders, the best balance between TM rights and the legitimate rights of others who may want to register names, and the most benefit to the trademark community at the lowest cost to them. In this paper we will initially examine the first two areas and their deficiencies, and then focus on the After-Launch (or ‘Takedown’) mechanism.

There has also been discussion on a fourth category which we will call ‘Limiting TLDs’. This is not a Rights Protection Mechanism per se, but rather an attempt to limit any TM impact of TLDs by limiting the TLDs themselves. In Appendix 1 we argue why this is a poor approach to Rights Protection, contrary to the objectives of the new TLD program, and problematic to implement.

1. Pre-Launch (‘Lists’)

We’ve heard various suggestions of RPM at Pre-Launch, all of which involve some kind of list (some call it “blacklist”, some say “white list”, we just say “List”). Possible eligibility criteria are marks that:

- A. meet certain criteria (registered in more than X countries, Y regions, and Z TLDs);
- B. have prevailed in more than X UDRPs;
- C. are themselves TLDs - to get on the List you have to get a TLD;
- D. are unique, distinctive, and/or made up;

The original list idea was that any string on the list could not be registered by anyone at the second level in any new TLD. List strings would be blocked/ removed from being able to be registered. This had problems because it may be that a trademark holder whose trademark string is on the list may want to actually use the name in the new TLD. For example, if “Verizon” is on the list, Verizon may actually want to use Verizon.phone, and Verizon would not be able to do that if the list is a block-list. Therefore, the list idea changed to where only the rights-holder can get the string in any TLD, and no one else¹.

There are five principal reasons why the List approach works poorly for TLDs:

1. There are classifications for trademarks and limitations for famous and well-known marks, but the List approach cannot uniformly apply these often litigated issues across different TLDs. For example, there are differences between .music and .family and what “famous and well-known” marks can be protected in each. The List cannot be uniform across TLDs because the TLD strings themselves are in drastically different commercial endeavors.
2. Trademark rights vary by nation, even for famous and well-known marks, whereas the DNS is uniform globally.
3. Fair uses for **all** trademarks exist.
4. It will be exceedingly difficult, politicized and controversial to select a methodology that decides which marks are on the list and which marks are not.
5. The List may be used in unanticipated ways such as in an infringement lawsuit unrelated to domain names or by governments during trade negotiations.

These are some of the reasons why a List of famous and well-known marks does not currently exist.

Some have suggested that a small List will be manageable and effective; however, there will be incredible pressure over time to expand it by loosening the eligibility criteria. It will become a constant source of dispute, controversy and political intervention (e.g. the initial List will unavoidably favor the marks of developed nations and pressure will be brought to ‘balance’ that). Trademark owners may simply perform the required activities to get on the List (e.g. file trademarks in multiple jurisdictions) even if there is no legitimate business reason for them to do so. Over time, management of the currency of the list will become a major and costly task.

Another significant flaw in the List approach is that it will not have a beneficial effect in .com, .net, .org or any existing TLD because these TLDs have all already had their launches. Yet those TLDs are where the vast majority of the trademark community problems occur and where most of the problems are likely to remain for the foreseeable future.

¹ Questions remain about names that are not on the list. For example, if a name is not on the list – does it lose standing in UDRP or ACPA disputes? For example if “windows” is not on the list, and someone registers windows.web, does Microsoft have less standing to complain? Should there be a list of strings that are generic and should not be on the list, even though the string may be trademarked in some class? For example, “blog”, “andrew” and “windows”.

We do not believe the cost (to the Internet community) versus the benefit (to the TM community) of a “List” RPM is worth it. Lists are not maintained by the U.S. Government (USG). The USG has opposed lists – whether they are geographic, famous, etc. – when negotiating international treaties and trade agreements. WIPO does not maintain Lists. A List is just not practical.

1. At Launch (‘Sunrise’)

By “at launch” we mean the first phase of name availability for registration. Various types of RPMs (usually called “Sunrises”) have been used at launch in the past. A sunrise is a period of time during which trademark holders have priority in registering their trademark strings before anyone else without a trademark can register any name (an example is the .info sunrise), or priority in making a ‘warning’ claim to the string before the name can be registered by anyone (an example is the .biz sunrise). The predominant reason cited by trademark holders for the need for a sunrise period is to “defensively register” their names. In other words – register them so that a cyber squatter cannot get the name later. Trademark holders typically say they do not use a sunrise to register names for actual use.

There are typically two phases to a sunrise. The first phase (the Validation Phase) verifies the identity of the TM rights holder and the validity of their claimed TM rights. The second phase (the Protection Phase) uses that information to block, notice, register or otherwise affect the status of the relevant second level name in the TLD (depending on the sunrise methodology chosen by the registry). Examples of different Protection Phase methods used in the past are in the ICANN Intellectual Property Constituency (IPC) paper titled “The Perfect Sunrise”.

We’ll refer to these two separate phases of Sunrise several times in this paper and so it’s important to understand their differences. The Validation phase is when the TM holder and their mark are authenticated. This can be done by any qualified entity. Performing in many ways like certificate authority, this entity validates that the trademark holder is who they say they are, and has the trademark they say they have, and it’s in the trademark office and class they say it’s in, etc. As we’ll discuss, there are good arguments to centralize this Validation function. The Protection phase is when second level domains are allocated to the trademark holder or otherwise protected. This phase can only be managed by the relevant Registry.

There have been several TLD sunrises in the past 10 years. Historically the Validation Phase is much more costly to the trademark holder (on the order of hundreds of dollars per name) than the Protection Phase (on the order of tens of dollars per name). With the introduction of a number of TLDs, we could obtain a significant efficiency gain if we (the community) centralize the Validation Phase. Trademark holders should not have to be validated at every registry but should only have to do this once. A central

Validation database system could capture and verify sufficient data about TM holders and their marks in order for all registries to make relevant, informed decisions during the Protection Phase. ICANN or another responsible party could run a procurement to select a qualified, competitive Centralized Validation Agency.

Although this sort of centralization/standardization would be very useful and efficient during the Validation phase, it is not feasible during the Protection Phase because all TLDs will not utilize the same Protection methodology. For example, .FAMILY may have a Protection phase of their sunrise that treats the trademark string “Andrew” differently than the .BERLIN TLD, the .IBM TLD, the .PERSON TLD, and the .WEB TLD. Since most of the costs for trademark holders are incurred during the Validation Phase, and most trademark holders will not register their names in all new TLDs (such as the more obscure or unrelated TLDs), the vast majority of efficiency gains will be realized by centralizing only the Validation Phase.

We understand why some trademark holders want a standardized approach to the Protection Phase. We at eNom have our own trademarks; “blog”, for example. It’s in a specific class, but we’d love to expand our right so we can demand “blog” at the second level in all new TLDs. However, we know that’s a land grab that would give us rights outside the law and would harm the needs and interests of legitimate registrants. If Microsoft applies for and obtains “.web” or “.msn”, for example, should our trademark on “blog” give us special rights to register “blog.web” or “blog.msn”? We think it shouldn’t.

Microsoft has a trademark on “Windows” but we do not think it has the right to preferred access to “windows.cleaning”. Similarly, McDonalds Corporation doesn’t have the right, in our view, to get preferred access to “mcdonalds.family”. We understand why Microsoft might want “windows.cleaning” – to prevent a registrant potentially infringing in the future. But the registrant has not infringed at the time of registration. Absolute Windows, Gutters & Pressure Washing Company (icleanwindows.net) has fair use for “windows.cleaning”. The McDonald family in Aberdeen, Scotland has fair use to “mcdonalds.family”. The law does not give these corporations (eNom included) preemptive TLD registration rights. A one-size-fits-all Protection Phase of Sunrise does not fit all. It harms registrants and registries and it goes beyond the intent and current application of trademark law.

So one might ask, why not have a mandated Protection Phase for each *type* (or category) of TLD? For example, community TLDs such as .MAORI and geographic TLDs such as .BERLIN might have one type of Protection phase, brand TLDs such as .IBM would have another, and open and generic TLDs, such as .WEB would have yet another. The problem with this approach is primarily with the open and generic TLDs. The TLDs .WEB, .FAMILY and .CLEANING will be open to any registrant because they are all generic TLDs – i.e. not restricted as to use or type of registrant in any way. They are open to any person or entity to register in them (just like .COM). The TLD “.FAMILY” is *not* closed to all but certified families. There is no entity or group that represents the community of families – it is not a “community” TLD. Still, McDonalds Corp does not have superior rights to register “McDonalds” in “.FAMILY” anymore than the McDonald family in Scotland does. The “.WEB” and “.FAMILY” TLDs are *both* gTLDs, yet, if they are

to have a “sunrise”, they should have the ability to choose a Protection Phase that suits their TLD, not be forced into one particular type.

The current draft RFP *requires* registries to have “*processes or mechanisms for the purpose of protecting legal rights of third parties by discouraging or preventing registration of domain names that violate or abuse another party's legal rights (“RPMs”)*”, **in addition** to the UDRP²”. This allows for innovation when it comes to RPMs. Our recommendation is that the TLD applicants choose from a number of pre-approved Protection Phase mechanisms (the IPC paper ‘Perfect Sunrise’ lists many) but that they may also propose their own, new and different mechanism. If the applicant chooses one of the approved types, there is no risk that their application will not pass that portion of the Initial Evaluation. If they choose their own, there is a risk.

In addition to all of the foregoing, a major deficiency of Sunrise (all phases) is that it is a ‘one-time’ solution. No matter what is implemented regarding RPM at At-Launch, it will not have an effect on existing TLDs such as .COM, because .COM has already launched. Also, if a new TLD becomes very popular after its Launch phase; its Sunrise will be in the past at that point and therefore it will be too late for any type of Sunrise mechanism to truly benefit rights holders. The real benefit to trademark holders comes after Launch, with a fast and inexpensive Takedown mechanism for clear trademark infringements.

2. After Launch - An “Expedited Takedown Mechanism”

We already have the UDRP but the framers of the UDRP did not include mechanisms like temporary restraining orders, preliminary injunctions, default judgments, or summary judgments. In this sense each UDRP goes to “full trial”. These trials are not fast, and they have the full costs associated with a trial -- even though the case may be obvious, or the defendant doesn’t bother to show up at the trial. We believe the system can be made more efficient in the majority of cases through the introduction of an ‘Expedited Takedown Mechanism’.

Expedited Takedown Mechanism (ETM)

The UDRP works well (WIPO recently described it as a “quick and cost effective procedure that has met with tremendous success”) but there are many cases where the infringement is so blatant, or the registrant so non-responsive, that a faster and cheaper method would be preferable. In addition to speed and cost, such a Takedown method would: a) better balance trademark interests with other, legitimate uses of trademarked words; b) reduce the ongoing need for full UDRPs; c) contribute to

² See #43 in the attachment to module 2, and attachment 7 of the applicant guidebook

more accurate Whois data; and , d) potentially be applied to .COM and other existing TLDs where the vast majority of trademark infringement is likely to continue to occur. Finally, Takedown is considerably more practical to implement.

The principle of a faster and cheaper take-down should have widespread support - but the details are all important. Recently Google said 57% of DCMA takedown notices (for copyright infringement allegations) are not legitimate and 37% are not valid copyright claims³. These invalid notices often come from businesses trying to undermine a competitor. This is one reason why the details of the domain-based ETM are so important. Another is that under the DCMA only a page or a small part of a site is taken down, but under an ETM the entire website is taken down. Our procedure must allow legitimate rights holders to take down blatant infringements, but disallow/discourage illegitimate Takedown actions from happening. As with the DCMA, the liability for a wrongful take-down must be with the complainant.

Our Proposed ETM

- 1) Complaint is via a bonded complainer
 - a. On the order of a \$500K bond (the cost to obtain such a bond will be below \$25K)
 - b. An **unlimited** number of complaints can be filed using the same bond
 - c. Anyone can put up the bond, including the complainant, but we anticipate existing corporate registrars and others such as law firms providing the bond as a service for their clients (complainants).
 - d. The rights holder would then file a complaint via the bonded complainer company (including details of the alleged infringement).
 - e. If the site is taken down and it is later found that the complaint was fraudulent or in error, the bond would be called to cover the damage to the registrant, if any.
Therefore, to reduce risk, the bond holder will be incented to pre-check the complaint. For example, they will ask "did the complaint come from a long-term existing client who we know is the holder of this trademark?"
- 2) There is a fee per name to Complainant
 - a. Call it \$200 - approximately 1/20th the cost of a UDRP
 - b. The bond holder might add \$50 to perform the service, for a total cost of \$250 to the Complainant
 - c. This fee limits frivolous or fraudulent complaining (and also covers the 'judges' costs) .
- 3) The complaint is assessed by a standing judge
 - a. The 'judge' could be in each registry or could be centralized with someone like WIPO or NAF. We think there will be more consistency of judgments if it is centralized.
 - b. The fee is to fund the judge's costs

³ See http://news.cnet.com/8301-1023_3-10200279-93.html?tag=mncol

- c. The judge uses the documentation to verify the identity of the complainant (e.g. is the complainant truly Microsoft Corp) and the validity of the claimed trademark.
 - d. There must be a live website.
 - e. The judge will determine if the website/domain name combination clearly and blatantly infringes the Complainant’s trademark.
- 4) If the judge believes there is a clear and blatant infringement, a notice is sent, using existing whois information, to the registrant (with an information copy to the registry and registrar)
 - a. If there is not clear and blatant infringement the Complaint is denied and the Complainant has recourse through the UDRP
 - 5) If there is no response from the registrant within a limited period (say 7 days)
 - a. Standing judge issues an RRP command to the registry to place domain on “Take Down” status (i.e. name servers are disabled)⁴
 - 6) If a response is received from the registrant
 - a. The Registrant must also pay \$200 – more information is acquired by the judge regarding identity of registrant and prevents volume squatters from gaming the system
 - b. Registrant response must include affidavit arguing their case to use of the name .
 - c. Standing judge makes decision – takedown or leave up – \$200 fee is refunded to the winner.
 - 7) A Complainant should have the ability to withdraw a Claim and the ability to ask the judge to ‘restore’ a name even though the Complaint was successful (in the event the Complainant subsequently finds out the registrant has legitimate rights – e.g. discovers there is a license between their company and the registrant)
 - 8) If complainant loses they always have option of proceeding to UDRP
 - 9) If registrant loses and wish to appeal they must file a ‘Reverse UDRP’ with WIPO for full and detailed consideration of the case

We don’t anticipate problems finding qualified, cost effective ‘Judges’. If the rules and processes are clearly defined – and we think they will be – and the threshold for Takedown is precise (“clear and blatant infringement of a trademark”) we think there will be a good supply of well qualified, motivated vendors for this service.

Although we have proposed many details above (e.g. bond amounts, fee amounts, durations,) these details are open to community discussion and amendment. What we are advocating in this paper is the overwhelming benefits of a Takedown process for clear trademark infringement - versus other possible RPMs which we think have significant conceptual and practical problems. The precise details of the Takedown process can be worked out in the weeks to come.

⁴ We envision the standing judge would be very similar to an accredited registrar, but in the judge’s case it can perform a *specific* (take-down) registry RRP command on any name at any registrar, while registrars can perform *any* RRP command, *but only* on names for which the registrar is the registrar-of-record for the name.

Some of the open questions are:

- a) What safeguards will be in place to prevent abuse of the mechanism?
- b) Who should pay and how much?
- c) How are notices sent (electronically or via another method)?
- d) How will liability be covered in the event of an error?
- e) Who will the 'judges' be?
- f) How can we get the mechanism agreed to and in place over the next several months?

We're confident the community can satisfactorily resolve these issues. Unlike a Lists approach, there are not that many variables to manage and we think there is a higher probability for strong consensus on the overall approach.

Summary of Benefits of Takedown RPM

- 1) With an inexpensive take-down for clearly squatted names, there is less incentive to squat.
- 2) All registrants have a strong incentive to maintain accurate Whois, because if they don't, their name is at risk for takedown (because they will not receive the notice from the standing takedown judge)
- 3) Bond holders have incentive to pre-verify complaints because their bond will be at risk for fraudulent or erroneous complaints.
- 4) For blatant infringement takedown is fast and cheap compared to UDRP, but not so cheap as to invite abuse. Also the UDRP remains available at any time
- 5) More information is obtained about the registrant because they need to pay a fee with their counter-notice.
- 6) The procedure can be expanded to cover other forms of abuse such as phishing and botnets⁵. Bonded complainers can include anti-phishing companies for example. In the case of an "immediate and credible threat to the internet", the standing judge could bypass the notice period, and the abusing names could be taken down immediately.
- 6) Procedure does not include registrars (in a decision making role); therefore "rogue" registrars cannot prevent takedown.
- 7) Procedure can be applied to .com with implementation of an ICANN "consensus policy"

⁵ Essentially formalizing the informal email lists and other informal procedures ICANN and registrars and registries use today when it comes to phishing and botnets.

3. Miscellaneous

Regarding RPM at the top level.

- A. We believe the need for defensive TLDs (at the top level) is very low because it is very unlikely that someone is going to spend \$185K minimum to, for example, try to get .MICROSOFT because the applicant would likely know they would lose the TLD and their \$185 K during the dispute phase. In the case of a TLD like “Windows,” if Microsoft is worried, then it could apply for .WINDOWS. It was Microsoft’s decision to use a descriptive word such as “windows” as a trademark. However, in our opinion, the risk is low that there will be a TLD application for .WINDOWS as rational applicants will not want to become involved in a dispute with large corporations who have well known trademarks. Also, if there were to be such a TLD application, in our opinion the chance is high the applicant would lose in the Objection phase.
- B. There needs to be a balance in terms of top level RPM, otherwise, the trademark owner for “sports” or “web” will have the right to get “.sports”, or “.web” (which are clearly generic terms).

Sanctions on Registries

In their 13 Mar 2009 letter to ICANN, WIPO proposes, among other things, a graduated series of sanctions on registries whose TLDs become ‘rife’ (our word) with trademark abuse. While there is some merit to this approach, the letter does not address the all important details such as ‘how much abuse,’ ‘to what extent is the registry liable’ and ‘at what point do various sanctions kick in’. We think these important details need to be fleshed out if this RPM method is to be seriously considered.

4. Conclusion

We strongly recommend an ‘Expedited Takedown Mechanism’ (ETM) instead of Lists or mandated Sunrise Protection phases. Expedited Takedown: 1) is the best balance between trademark interests and other, legitimate uses of trademarked words; 2) reduces the ongoing need for UDRPs, which are a large cost to trademark holders; 3) contributes to more accurate Whois data with accompanying benefits in many areas of domain management; 4) is the only method that can be also applied to .COM (where the vast majority of trademark infringement will likely continue to occur); 5) has been proven to work in many ccTLDs; and 6) is the most practical method to implement given the deficiencies of the other methods.

If there is a required Sunrise for new TLDs we see efficiencies in separating the sunrise into two phases. In the first phase, the Validation Phase, there should be a centralized repository of authenticated and verified TM holders and their marks. This would prevent trademark holders from having to be authenticated multiple times at multiple registries (with accompanying cost and consistency benefits). The second phase, the Protection Phase, would allow registries to use this authenticated data to allocate or otherwise protect trademark strings in accordance with their TLD-specific policies. Registries should choose or develop the Protection Phase method that best suits their TLD, even though the TLD may be open and generic.

Finally, we need to strongly resist efforts to restrict the number or type of TLDs (in the context of 'type' we mean efforts to only allow TLDs for communities, brands, IDN or authenticated membership). Such limitation is not a RPM and will result in TLDs which do not bring innovation and competition to the world's internet. This round is about generic TLDs and competition, not restricted or hobbled TLDs. We should concentrate on real and effective RPMs, not on restricting new TLDs.

Comments and feedback welcome at paul.stahura@enom.com or richard.tindal@demandmedia.com

Appendix 1.

Why Limiting the Number or Type of TLDs is a Poor Rights Protection Mechanism and Bad Policy

Arguments have been made that limiting the number of TLDs (e.g. to no more than 20) or the type of TLDs (e.g. 'Community', brand or IDN TLDs or only) will be beneficial to TM interests. We do not view such limitations as a legitimate RPM. We think such approaches are contrary to the objectives of the new TLD process, impractical to implement in a fair manner and, obviously, inapplicable to existing TLDs.

Competition is Key Objective. As stated in ICANN policy documents, and the Joint Project Agreement between ICANN and the US Government, the primary objective of this round is to introduce competition. Previous rounds of TLDs limited applicants in various ways (number, type, operating rules, pricing). When limitations are placed on applicants their ability to compete is constrained. In our view, this is the major reason why TLDs introduced since 2000 have failed to effectively challenge .COM, or bring significant innovation to the domain industry. This round of TLDs has been designed to minimize constraints on new TLDs (beyond the necessary technical and business standards imposed on the applicants). Therefore, this round has the best potential to create TLDs that introduce genuine competition by virtue of their attractive strings, marketing plans and/or innovative functionality. Limiting TLDs to those with restrictive rules and discrete communities (e.g. the BOYSCOUTS), as opposed to truly open TLDs, such as .HIKING, will create TLDs that are not able to generate broad consumer

interest and benefits. In short, TLDs that cannot effectively compete with existing TLDs (or with each other). Similarly, limiting TLDs to only .IDN will constrain the full effect of market competition. It will have negative impacts on competition, jobs and investment in regions where the Latin alphabet is used. Creating purely 'silos' of TLDs via Community, brand, etc will not introduce genuine completion.

Limitations Create Unfairness Limitation by applicant type will significantly favor certain groups whose characteristics fulfill the basis of limitation. These groups will be awarded TLDs whereas other types of applicants will not. It will also create gaming behavior in which other applicants try to tailor their proposal to suit the limiting factors. And again, what is a fair and competitive basis to pick and choose winners?

Limiting TLDs by Having Authentication Rules Can Harm Registrants. A further method of limiting TLDs is to require pre-registration validation, such as verifying the validity of the registrant's identity and whois information. This is very costly. It would impose dramatically increased prices and time delays on compliant (non-infringing) registrants and could be defeated by bad actors through the use of stolen identities or temporary contact details.

Limiting the Number of Applicants is Not Practical. We can think of no fair and practical way to limit the overall number of applicants. First-Come-First Served would strongly favor applicants with the best automated scripts and the most connections to the TAS application system. Typically this will be domain industry 'insider' companies.

Limitation by random selection of applicant slots will cause applicants to apply for many more slots than they normally would in order to maximize their chances of selection. Assuming there is a fee per applied slot, this will result in well funded applicants receiving the lion's share of TLDs (there may also be illegal lottery implications). Similarly, limitation by the auctioning of slots will result in TLDs only being awarded to well- funded applicants.