New Generic Top-Level Domains: Trademark Protection, Malicious Conduct Mitigation

WIPO

12 October 2009

Purpose and Agenda

- As the introduction of new top-level domains becomes imminent, ICANN is holding a series of discussions focusing on:

  - ↕ Protections for trademark holders

  - ↕ Prevention and mitigation of malicious conduct

- Proposals published for discussion & possible inclusion into the new gTLD Applicant Guidebook (www.icann.org)

- Agenda: (1) Background
            (2) Rights Protection
            (3) Malicious Conduct Mitigation

ICANN

ICANN Formation and New gTLDs

- A core objective in founding ICANN; a requirement in each ICANN MoU with the USG:

    "Define and implement a predictable strategy for selecting new TLDs"

- Fostering choice and competition in provision of domain registration services

- White Paper,1998: "The new corporation ultimately should … oversee policy for determining the circumstances under which new TLDs are added to the root system"

ICANN

ICANN Policy Development Process

- Policy development process by ICANN's Generic Names Supporting Organization (GNSO)
  Dec 2005 – Sep 2007

- Terms of Reference (questions to be answered):

  - ↕ Whether to introduce additional gTLDs

  - ↕ TLD string selection criteria

  - ↕ TLD allocation methods

  - ↕ Contractual conditions

- Policy embodied in 19 separate recommendations

ICANN

Policy Conclusions

- New gTLDs will benefit registrant choice and competition

- The implementation plan should also allow for IDNs at the top level

- Introduction of new gTLDs should not cause security or stability issues

- Protection of various appropriate interests requires objection and dispute resolution processes

ICANN

Principles of the Implementation Process

- Care/conservatism: protection of registrants, DNS stability and security is paramount.

- Application proceeds are planned to cover costs.

- ICANN will provide a clear, predictable, timely road map for the application, evaluation and delegation of gTLD strings.

- Some applied for strings should be excluded through an independent objection process, if they:
  - ↕ clearly incite certain malicious conduct,
  - ↕ are an infringement of rights,
  - ↕ are a misappropriation of a community label, or
  - ↕ create user confusion

ICANN

Trademark Issues

- "TLD strings must not infringe the existing legal rights of others that are recognized or enforceable under generally accepted and internationally recognized principles of law." [GNSO Policy]

- "While [new gTLD] entry generally promotes consumer welfare, proper account also must be taken for property rights that protect firms' investments in establishing a reputation and brand name." [Dennis Carlton]

ICANN

Existing trademark protections in use

There are several solutions in place currently in the marketplace

- Rapid take down occurs in case-by-case manner

  ↕ At registries (ccTLD and gTLD)

  ↕ With ICANN / registrars / registries

- Online trademark registries exist in many jurisdictions

- Sunrise periods - IP clearinghouses used by: ccTLD (.eu) and gTLD (.asia) launches

The IRT (and others) have considered some form of standardization of potential solutions in their work

ICANN

WIPO / ICANN: On-going Collaboration

- Extensive discussions regarding pre-delegation legal rights objections process and standards

- WIPO to serve as dispute resolution provider for legal rights objections

- WIPO proposed Right's Protection Mechanisms:

  - ↕ post-delegation dispute resolution

  - ↕ expedited suspension mechanism (ESM)

- WIPO participated in IRT discussion and public discussion

ICANN

Trademark Issues Solution Development

- IRT formed by the Intellectual Property constituency at the request of the ICANN Board,

- The IRT developed Preliminary and Final Reports recommending seven specific solutions,

- Discussion of solutions: online comment forum, consultation sessions in Sydney, New York and London,

- Synthesis: proposed solutions published

ICANN

Proposed Rights Protection Mechanisms

- IP Clearinghouse – a database of validated trademarks to be utilised by new gTLD registry operators during launch in implementing either an:

  - ↕ IP Claims service or

  - ↕ Sunrise process during TLD launch

- Uniform Rapid Suspension process – for use in clear-cut, blatant cases of trademark infringement

- Requirement for Thick Whois database maintenance

- Post-delegation enforcement

ICANN

Post-delegation Rights Protection

- Designed to combat

  - ↕ Registry Operators that operate a TLD in a manner that is inconsistent with the representations and warranties contained within its Registry Agreement,

  - ❼ Contractual Compliance audit & investigation

  - ↕ Registry Operators that have a bad faith intent to profit from the systemic registration of infringing domain names

  - ❼ Post-delegation dispute process

- Possible remedies: Graduated sanctions / suspension

ICANN

Malicious Conduct Mitigation

The following groups or representatives of these groups have participated in the development of issues and solutions in this area:

- APWG (Anti-phishing working groups)

- BITS (A division of The Financial Services Roundtable)

- MyCERT (Computer Emergency Response Team, Malaysia)

- FIRST (Forum of Incident Response and Security Teams)

- RISG (The Registry Internet Safety Group)

ICANN

Malicious Conduct Issues identified

A. How do we ensure that bad actors do not run Registries?

B. How do we ensure the accuracy, integrity and validity of registry information from the TLD to the end-user?

C. How do we provide enhanced control framework for TLDs with intrinsic potential for abuse?

D. How do we provide an improved framework for combating abuse?

ICANN

Proposed Malicious Conduct Mitigations

1. Enhanced requirements and background checks

2. Disclosure of previous involvement in UDRP process

3. Demonstrated plan for DNSSEC deployment

4. No wildcarding/remove glue records

5. Elective TLD security designation program

6. Requirement for thick Whois

7. Publish anti-abuse contact and suspension procedures

8. Expedited Registry Security Request process

TLD Security Verification

Elective verification program for TLD's to establish, measure and demonstrate an effective security program

- Requires TLD-Registry and its Registrars to design and operate a defined standard of security and operational controls

- Establishes a common standard and language for TLD security and operational control that can be measured

- Provides a mechanism and structured approach to enhancing security and operational control within a TLD

ICANN

THANK YOU

Kurt Pritz, ICANN

pritz@icann.org

ICANN