International Trademark Association
Representing Trademark Owners Since 1878

INTA Internet Committee Comments on
HSTLD Advisory Group Program Development Snapshot
April 8, 2010

I. Introduction

The Internet Committee of the International Trademark Association ("INTA") appreciates this opportunity to comment on the High Security Zone TLD Advisory Group's ("HSTLD AG") Draft Program Development Snapshot (the "Snapshot").[1]

As ICANN is well aware, the problems associated with phishing and other types of malicious conduct utilizing domain names are a serious threat to the stability and security of the Internet and Internet users' trust. For instance, the Anti-Phishing Work Group reported that for the 4th Quarter of 2009 there were more than 130,000 unique phishing websites detected.[2] The Committee applauds the HSTLD AG's efforts to develop a program and enforcement mechanisms to support control standards and incentives that will increase trust in TLD's participating in the HSTLD program. However, the Committee believes that the overarching issue of malicious conduct in new gTLDs will not be addressed unless the HSTLD program is modified, a level of mandatory participation in the program is required, and the DAG is further revised to address the comments and concerns raised by the community.

The Committee is encouraged by the HSTLD AG's efforts to assemble a set of principles, processes and controls that will be seen as "best practices" for the operation of a safe, secure and trusted high security TLD. Of particular importance to the Committee are the requirements relating to Whois service levels (Principal 1.2), the thick Whois process and support (Principal 2.4), the establishment of controls to address malicious conduct (Principal 2.4), the verification of registrant identity (Principal 3.1) and the registrar's confirmation of accurate registration data (Principal 3.2). The Committee looks forward to participating in the development of meaningful criteria and controls that certify these important objectives. The Committee, however, cautions against a self-certification or report card program because of its inherent lack of transparency and controls. Additionally, the HSTLD program should not serve as an alternative platform used to scale back rights protection mechanisms and important security policies and procedures or to move them from the Draft Applicant Guidebook to this voluntary certification program.

II. Support for More Reliable and Accurate Whois Data

Under the current system, Whois data for domain names being used for malicious conduct or the infringement of intellectual property rights is frequently inaccurate. The Snapshot's proposal to add stronger Whois identity verification for HSTLD registrants is necessary in order to protect the public and brand owners against instances of infringement and malicious conduct.

---

[1] Available at http://www.icann.org/en/topics/new-gtlds/hstld-program-snapshot-18feb10-en.pdf

[2] Phishing Activity Trends Report, 4th Quarter 2009. Report available at http://www.antiphishing.org/reports/apwg_report_Q4_2009.pdf

In fact, the current lack of policing relating to accurate Whois data creates such a significant barrier to the enforcement of rights that the Committee considers a Thick Whois system an imperative to the HSTLD program. As the IRT noted in its Final Report, the thick registry Whois model has been employed in many new gTLDs for many years without any evidence of legal problems.[3] For this reason, the Committee supports the Snapshot's efforts to establish effective controls to reduce malicious conduct by requiring that registrant's within a HSTLD domain supply detailed and accurate registration information and that registrars and registries agree to police and enforce such requirements. Furthermore, one prerequisite for HSTLDs' credibly as zones in which users can be assured that the site they deal with is what it seems, is prohibiting private registrations in HSTLDs.[4]

III. HSTLD Certification and Measures to Reduce the Incidence of Malicious Conduct

The auditing of HSTLD registries, registrars and registrants is essential to earn the trust of Internet users and the reputation necessary for an effective certification mark. In fact, in order for a mark to qualify as a certification mark under United States law, the owner of the mark must "legitimately exercise control of the mark." 3 J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition*, § 19:92 (4th ed. 2009). As a result, the audit processes and enforcement mechanisms for ICANN to certify a registry as a "High Security TLS" will be paramount. The Committee urges ICANN to develop and set forth for comment a proposed audit process and a description of how the HSTLD program will be staffed and funded.

In addition to setting forth the processes and controls necessary for a valid certification mark, the marketplace of Internet users will ultimately determine the usefulness of the HSTLD certification. In other words, if the consuming public is not aware or does not understand the certification mark, then businesses and brand holders will have no incentive to follow Internet-users to a high security TLD. One of the practical issues that came up during the Committee's review and discussions of the HSTLD program was the possibility that the HSTLD certification be readily identifiable by Internet users through integration with the user's browser. At a minimum, the Committee suggests that a user-friendly and quick way to identify a domain name within the HSTLD be designed.

---

[3] See, http://www.icann.org/en/topics/new-gtlds/irt-final-report-trademark-protection-29may09-en.pdf; See also, http://www.icann.org/en/announcements/announcement-18dec07.htm

[4] For greater detail on the lack of registry compliance with Registrar Accreditation Section 3.7.7.3 provision for accurate Whois contact information, see April 24, 2009 letter from IPC to Doug Brent, http://www.icann.org/correspondence/metalitz-to-brent-24apr09-en.pdf. Also, as discussed in the IRT Report, although privacy concerns have been alleged with respect to a Thick Whois model, the model poses no additional privacy concern (as compared with Thin Whois) other than the possession of the data by one additional party (the registry) whose bona fides have been vetted during the registry application process. Moreover, no registry has invoked the ICANN procedure put in place to address conflicts between Thick Whois data collection and national privacy laws. See, http://www.icann.org/en/topics/new-gtlds/irt-final-report-trademark-protection-29may09-en.pdf, at p. 46.

IV. Report Card Concept Unlikely to Achieve a Sufficient Level of Control and User Trust

The Snapshot introduces the concept of self-reporting supported by a security "Report Card." The Report Card lists a number of security control criteria and uses different colors to reflect self-reported compliance, verified compliance, or non-compliance. The Committee believes that the Report Card concept is too complex to be useful and that self-auditing will undermine the usefulness of HSTLD's.

First, the public will not value an HSTLD certification that requires a "closer look" to determine if security is truly high, and indeed a complex or unintuitive certification may be counter-productive or misleading. The Committee believes that high security will need to be a binary concept to be useful to consumers: either a TLD has met ICANN's objective criteria for heightened security or it has not. Most Internet users will not take the time to explore the data behind a certification or seal, and even those who do may not appreciate the implications of self-reporting. Accordingly, we believe the Report Card concept is flawed and should be reconsidered.

Next, the Committee submits that the name "high security" implies something more than self-auditing, which may or may not be performed in a diligent manner. Self-reporting will inevitably open the door for some registries to cut corners. The ineffective nature of such a self-auditing system is illustrated by the widespread problem of inaccurate Whois data, which is not meaningfully audited by registries or registars.[5] Therefore the Committee believes that regular, independent certification is essential to the credibility of HSTLD's.

Lastly, the Committee supports greater identity verification for domain names in all TLD's, and has advocated some level of mandatory participation in HSTLD to achieve this. The Committee is concerned that an entirely voluntary system will not reach critical mass, and will not be able to sustain an independent certification authority. Short of fully mandatory participation, the Committee supports two possible approaches:

- a framework requiring mandatory participation in limited fields, such as fields involving financial subject matter (e.g., ".bank"), young audiences (e.g., ".kids"), gTLDs that have reached a threshold of dispute proceeding or proxy registrations, or any gTLD that represents implicitly or explicitly that it has enhanced security (e.g., ".safe"); or

[5] The Whois Data Problem Report System (WDPRS) which ICANN developed to allow third parties to report Whois data problems is concrete evidence of the ineffectiveness of a self-auditing procedure. As reported by ICANN in its December 2009 Contractual Compliance Semi-Annual Report, during the period from December 19, 2008 to December 7, 2009, ICANN received a total of 52,572 WDPRS reports on which registrars were required to investigate and take action. Of the 50,981 45-day follow-up notices sent, ICANN only received back 21,965 responses (i.e., less than 50% response rate). Further, of the 10,008 subsequent ongoing inaccuracy claims, registrars took action on only slightly more than 50 percent of them. With such results, the thought that registries and registrars can police themselves is completely unrealistic. See, http://www.icann.org/en/compliance/reports/contractual-compliance-report-24dec09-en.pdf

- a specific preference in awarding gTLD's to applicants that agree to verify identity and prohibit masking[6].

The ease with which one can currently maintain anonymity when registering a domain name allows unscrupulous individuals to mislead the public and practice fraud and trademark infringement on an unprecedented global scale. We believe enhanced identity verification for all gTLD's is needed to avoid further erosion of public confidence in the authenticity of branded goods and services offered on the web.

V. Recommendation that the HSTLD AG Focus on Identifying Benefits for Brand-owner Registrants and Internet Users

The Snapshot lists a number of benefits that may be realized by the implementation of an HSTLD program. The Committee agrees that many of the benefits set out in the Snapshot would improve Internet security and would benefit registries, registrars, registrants and end users.

In particular, the Committee agrees that domain name registrants would benefit from increased security and verification mechanisms, and mechanisms which empower registries and registrars to take action against breaches of terms of service and against malicious conduct. The Committee also agrees that both registrants and Internet users will benefit from verified registration data and a reduction in incidence of malicious conduct.

Recognizing that the proposed list is not a comprehensive business benefit analysis, the Committee suggests that further work be done to provide a more robust list of the practical benefits registrants and end-users may see from high security zone certification. The Committee is also of the view that the HSTLD AG consider the manner in which an HSTLD certification program would be marketed to such end-users to increase the likelihood of marketplace adoption of high security TLDs. A failure to clearly communicate the benefits of registering domains in high security TLDs (and in doing business with companies whose domains are so registered), will likely mean that the program will generate little interest (particularly if registration of such domains is more expensive than registration in "non-secure" registries). The Committee suggests that an incentive or business benefit would be to propose that new gTLD applicants that agree to be part of the HSTLD program be awarded more points in the application process.

Thank you for considering our views on these important issues. Should you have any questions regarding our submission, please contact INTA External Relations Manager, Claudio Digangi at: cdigangi@inta.org

About INTA & The Internet Committee

The International Trademark Association (INTA) is a more than 131-year-old global organization with members in over 190 countries. One of INTA's key goals is the promotion and protection of trademarks as a primary means for consumers to make informed choices regarding the products and services they purchase. During the last decade, INTA has served as a leading voice for trademark owners in the development of cyberspace, including as a founding member of ICANN's Intellectual Property

[6] Recently, the .RU registry adopted a registrant verification policy that will require individuals and businesses applying for a .ru domain address to provide a copy of a passport or legal registration papers. See http://gigalaw.com/2010/03/22/russia-to-verify-identities-for-domain-registrations/

Constituency (IPC).

INTA's Internet Committee is a group of over two hundred trademark owners and professionals from around the world charged with evaluating treaties, laws, regulations and procedures relating to domain name assignment, use of trademarks on the Internet, and unfair competition on the Internet, whose mission is to advance the balanced protection of trademarks on the Internet.