Brand Registry Group Comments in Response to Competition, Consumer Trust and Consumer Choice Review Team - New Sections to Draft Report of Recommendations

15 January 2018

The Brand Registry Group (BRG) welcomes the opportunity to provide comments in relation to the new sections of the draft report issued by the Competition, Consumer Trust and Consumer Choice Review Team (CCT).

Our members are applicants, including future applicants, and operators of dotBrand registries. The new gTLD program was valued by our members because of the opportunities that it brings to businesses, where domain names can be sign posts to authentic goods and services, providing trusted spaces on the Internet and safeguarding end users.

A dotBrand operator controls the end-to-end functions from managing the registry operations through to delivery of online services via their top-level domain registry. As a result of this distinct operating model, it is extremely unlikely that a dotBrand registry would experience DNS abuse in their TLD, due to the fact that the registry operator has a direct relationship with the registrant (it is the same, an associate or a licensee) and does not distribute domains to third parties. Similarly, wilful infringements against trademarks in relation to domain names registered in a dotBrand TLD are unlikely to occur.

With over 500 dotBrand registries now in operation since the new gTLD program was launched, it is not surprising that these have been free from DNS abuse with no reported incidents.

BRG Comments

Comments on Chapter 5 - Safeguards, Recommendation A: Consider directing ICANN org, in its discussions with registries, to negotiate amendments to existing Registry Agreements, or in negotiations of new Registry Agreements associated with subsequent rounds of new gTLDs, to include provisions in the agreements to provide incentives, including financial incentives, to registries, especially open registries, to adopt proactive anti-abuse measures.
The BRG welcomes the promotion of activities to prevent and mitigate DNS abuse. However, this recommendation appears to ignore registry operators that have invested in and implemented pro-active anti-abuse measures and/or those that have inherent safeguards built into their registry model, such as dotBrand and highly restricted registries. Providing financial incentives to operators that do not have existing proactive measures is not an equitable approach and is at the detriment of those that already maintain safeguards. An alternative approach could be incentivise registries that have already implemented pro-active anti-abuse measures, or where these are inherently "built-in" to the registry model. This will ensure operators maintain these measures and encourages others to adopt the same.

Comments on Chapter 5 - Safeguards, Recommendation C: Further study the relationship between specific registry operators, registrars and DNS abuse by commissioning ongoing data collection, including but not limited to, ICANN Domain Abuse Activity Reporting (DAAR) initiatives. For transparency purposes, this information should be regularly published in order to be able to identify registries and registrars that need to come under greater scrutiny and higher priority by ICANN Compliance. Upon identifying abuse phenomena, ICANN should put in place an action plan to respond to such studies, remediate problems identified, and define future ongoing data collection.

The BRG shares the concerns of the Registry Stakeholder Group which has been raised in their comments and is copied below for ease of reference:

RySG comment on new recommendation

The RysG supports the recommendation that ICANN conduct ongoing research on DNS abuse, but cautions against using the DNS Abuse Study to come to any conclusions and strongly opposes the use and publication of data from DAAR.

While the RySG respects the intent and efforts of the researchers who conducted the DNS Abuse Study, the RySG believes the study is flawed and it should not be the basis for any decisions. These flaws include: The study is self-referencing and in many cases only references prior work by the same authors (see the Reference list in the study where the authors repeatedly quote themselves). The study makes conclusions for which it provided no data or analysis in the text (despite no data about price, and only mentioning price twice as a sidenote, the study concludes that lower prices might be linked to abuse). The study circularly relies on the statements of the tools it chose to use, (i.e. citation to Spamhaus itself for its assertion that Spamhaus is a "near zero false positive list").

The RySG is not opposed to ongoing anonymized data collection to learn more about abusive behaviors but strongly recommends that the researchers chosen be required to provide clear reports that link every conclusion to a specific data point and analysis. Even though the RySG does note that the report contains some positive, and well-researched findings based on data (such as the findings that most new gTLDs are not havens for abuse or malware), the quality of the study is lacking enough that care should be taken when interpreting all of the results.

Furthermore, as mentioned previously, ICANN has created DAAR behind closed doors, with no community consultation, and determined which 3Ps data feeds it will rely on, without input from the community. ICANN has apparently, in determining how "trusted" these 3Ps are, relied on the cost-benefit-risk analysis of corporate IT departments that pay for filtering rather than the needs and interests and concerns of the community, and particularly contracted parties. Although there is much benefit to be had in establishing reliable tools for the measurement and mitigation of abuse, which it is assumed is the ultimate aspiration for the DAAR project, any current reliance on DAAR is exceptionally premature.The CCT-RT should not recommend use of DAAR to monitor or police contracted parties, until the community has had a chance to discuss and debate the impact, benefits and risks to the various constituencies. In particular, the CCT-RT should not recommend that ICANN publish the data from DAAR until there is a mechanism in place for addressing community concerns that does not jeopardize the reputation or business of the RO without a fair and impartial investigation, and ICANN acknowledges its potential liability for reliance on DAAR.