Comments of GNSO Intellectual Property Constituency (IPC)

July 20, 2009

IPC appreciates this opportunity to comment on some of the "excerpts" for version 3 of the Draft Applicant Guidebook, and on certain explanatory memoranda, released by ICANN on May 31, 2009. See http://www.icann.org/en/topics/new-gtlds/comments-e-en.htm#matrix. Since ICANN staff has labeled most of the proposed changes for incorporation into version 3 as "interim language," these comments are not meant to foreclose further IPC comments on the same topics when the full text of DAG version 3 is released.

I. Module 2: Geographic Names

IPC accepts in principle the concept of safeguards against use at the top and second levels for certain country and territory names, identified through objective criteria, even though these names do not enjoy specific protected status under international treaties. We note that the concept is fundamentally the same as the one underlying the Globally Protected Marks List proposed by the Implementation Recommendation Team.

We also note that in proposed paragraph 2.1.1.4.1.g, safeguards would also apply to "permutations or transpositions" of the country names. While examples are given of "permutations," none is supplied for "transpositions". It is difficult to evaluate the scope and impact of the proposal without a further explanation of these terms. If a broad interpretation were given to these terms, it could improperly expand the scope of the safeguards.

II. Module 2: Evaluation Criteria

(A) Applicant Background (questions 11(a)-(f)): IPC applauds the proposal to require greater transparency regarding new TLD applicants. Bad actors, and in some cases even criminal elements, have become ICANN-accredited registrars or have been allowed to operate gTLD registries; it is critical that this not be allowed to happen in the new gTLD space. The drafted questions should be carefully reviewed, and broadened where necessary, to ensure that they will capture the needed information. For instance:

- Information should be requested regarding all partners of an applicant that takes a partnership form;
- ICANN should inquire about criminal or fraudulent activities of the officers of entities (e.g., corporations) that hold a significant interest in the applicant;
- Criminal record disclosures should not be limited to financial or fiduciary related crimes, but at a minimum should cover all felonies;
- Disciplinary actions by governments should not be limited to those imposed by the relevant person's or entity's domicile;

- Question 11(f) should be rephrased to cover all allegations of intellectual property infringement "in connection with the registration or use of" a domain name;

- The notes should spell out that all applicants will be subject to a background check, and that false, misleading, or materially incomplete responses will be grounds for rejection of the application.

(B) Community-based designation (question 24): These questions should provide greater transparency and detail regarding claims of community status. That should enable potential objectors to make more informed decisions about whether to invoke the community objection procedure, as well as facilitating the comparative evaluation/community priority process, if applicable.

(C) Security policy (question 36): IPC commends ICANN for recognizing, as this questions does, that "due to the nature of the applied-for gTLD string," some applicants may be expected to meet higher security standards than would be the case for other, less sensitive strings. We are also pleased to see the observation that "certain financial or industry-oriented TLDs" may require stronger safeguards. For example, we believe this category should include TLD strings referencing industry sectors associated with high levels of online intellectual property infringement, and that the security and other policies of applicants for such strings should be expected to include adequate safeguards against such illegal (and in some instances criminal) activities. In any event, the criterion that the applicant demonstrate "security measures appropriate for the applied-for gTLD string" is an important and potentially valuable addition to the evaluation process.

(D) Whois (question 38): ICANN should also take this opportunity to provide incentives for the new registries to take on some of the responsibility for ensuring that the ICANN-accredited registrars which they employ to sponsor registrations live up to their obligations with regard to Whois. Registries should also be encouraged to require that their registrars take proactive steps to improve the accuracy of Whois data; that they consistently cancel the registrations of those supplying false Whois data; and, if they provide proxy or private registration services (to the extent the registry allows them), that they include and implement a process enabling copyright or trademark owners who present reasonable evidence of actionable harm to obtain access to the actual contact data of registrants. Registries that commit to these policies should receive extra points in the evaluation process.

III. Module 3: Dispute Resolution Procedures

A. Morality and Public Order objections/ Independent Objector

IPC urges ICANN to approach this concept with caution. Broad standing to raise morality and public order objections throws the door open to challenges being filed on specious grounds or for purposes of harassment. Standing requirements that are moored to consideration of injury or potential harm to the complainant are less vulnerable to such abuse. While ICANN is considering a process for screening out frivolous objections, it could be indispensable in this situation. It is not clear whether there would be any penalty for filing a frivolous morality and

public order objection that is rejected at the initial stage. Because of the high potential for abuse, and the potential chilling effect of morality and public order objections on controversial communications, ICANN should consider how to penalize complaints deemed frivolous on initial review, such as by forfeiture of the filing fee.

ICANN should also be mindful that even non-frivolous morality and public order objections could be brought for purposes of harassment or suppression of speech. For example, a non-frivolous argument could be made that allowing a gTLD like <.kurdistan> is detrimental to public order if it might incite violent lawless action. However, such an objection may be a pretext for suppressing political speech on rights and self-determination. The possibility of abuse counsels for defining standing grounds narrowly rather than broadly, as a means of reducing bad faith but non-frivolous claims to the extent practicable. The Independent Objector is empowered to take action against "highly objectionable" gTLD applications on morality and public order grounds, which should act as a sufficient check on obviously problematic gTLDs (like derogatory terms for ethnic groups).

B. Community Objection

IPC appreciates a number of the clarifications that ICANN proposes to make in section 3.4.4, including language that spells out that a "community" may be composed of legal entities (including business groups), not just individuals. However, one overarching problem with the community objection criteria is the definition of the "detriment" that an objector must show. "Detriment" evidently does not include the harm that may result from granting another party exclusivity in the proposed community-based gTLD string.

While we recognize that this is not strictly a trademark law issue, trademark precedents can be instructive here. Most trademark laws allow oppositions to be brought on the grounds that a term for which trademark protection is sought is descriptive or generic, because allowing one party to claim exclusivity in such terms could have an adverse impact on other parties. Such oppositions do not require showing that the applicant actually plans to enforce its mark in a manner that would cause such an adverse impact; the mere fact of exclusive appropriation is viewed as sufficient. The current rules do not appear to take into account the detriment that may come from granting exclusivity, particularly in the situation where multiple parties may be able to claim to speak for significant portions of the community. Any representative institution with sufficient standing to bring an objection should be rebuttably presumed to risk suffering detriment if the challenged TLD is awarded to the applicant.

The detriment requirement should also be clarified to address cases where the objection is based either on the applicant's lack of standing to represent the community or the legitimacy of the community definition itself. In such cases, a complainant may not be able to show "detriment" in the way Section 3.4.4. defines the concept, but it should not matter. Indeed, the community definition and the applicant's eligibility to represent the community are threshold issues that should be subject to review on a complaint from any party that has a good faith belief that it would be harmed, whether or not that harm falls within the enumerated "detriment" categories in Section 3.4.4.

We commend ICANN for proposing the changes in the excerpts to the "complete defense" discussed at the end of section 3.4.4, especially clarifying that the applicant has the burden of demonstrating this defense, and ensuring that it cannot be invoked by an "open TLD" applicant. However, we urge that it be further reviewed. By giving an absolute defense to a community applicant who can show standing (for purposes of a hypothetical challenge to another hypothetical application), the rules are much too strongly biased toward granting the gTLD to the first to apply for it, a result that could end up harming the communities the rules purport to protect.

Finally, the proposed changes do not address procedural problems with the community objection process, including doing more to encourage consolidation of objections filed by the same party against multiple applicants, publishing a running list of objections received, and providing greater predictability on fees.

IV. Module 3: Explanatory Memorandum: Registry Restrictions Dispute Resolution Procedure

There is certainly some value in providing a channel through which third parties can object to the failure of a community-based registry to enforce its stated restrictions on who can register, what second-level strings they can employ, and how they can use domains in the TLD. However, as set forth by ICANN, this proposal raises a number of questions as well. For example:

- Why would the procedure be restricted to community-based TLDs? It is quite possible that an application which is never designated as community-based will also include restrictions in these areas. One example would be a TLD designed to accept only registrants who are employees, customers, or suppliers of a single company. In the typology that ICANN has consistently proposed throughout this process, there could be many instances in which the registration or use rules of an "open" TLD would be far more restrictive than those which the applicant has unilaterally chosen to designate as a "community" TLD. Why should only the latter be subject to an RRDRP requirement?

- Would the availability of a standardized RRDRP relieve registry operators of the responsibility to enforce the stated restrictions themselves, or undermine their incentive to provide customized enforcement mechanisms (such as registry-specific procedures to challenge the eligibility of registrants)?

- Since the restrictions in question would be set forth in an enforceable agreement between ICANN and the registry operator, is it appropriate for ICANN to abdicate any responsibility for enforcing that agreement, instead turning the job over to third parties (even if the contract formally denies them any status as "beneficiaries" of the contract)? This temptation would be particularly strong if the RRDRP provider were empowered to impose remedies such as graduated sanctions, or even forced re-delegation, that would ordinarily be within the purview of ICANN. It is one thing for an RRDRP to be available as a supplement to ICANN contract compliance activities; it is quite another thing for the RRDRP to become an incentive, or even an excuse, for weak ICANN compliance and audit efforts.

- How would an RRDRP be integrated with other post-delegation remedies, such as the procedure proposed by the Implementation Recommendation Team for use with registries that fail to live up to other representations made in the application and/or enshrined in the registry contract with ICANN?

V. Module 4: Comparative Evaluation Criteria

The disaggregation of the scoring criteria is an improvement and makes the overall process easier to understand. IPC also supports the concept of lowering the threshold that must be met (13, rather than 14, of a possible 16 points) in order to survive what is now called the "community priority" evaluation, and thus avoid having the TLD string allocated by auction. (IPC reiterates its strong concerns about auctions as a mechanism for awarding new gTLDs [see http://www.ipconstituency.org/PDFs/IPC%20comments%20on%20auctions%20paper%20090708.PDF and previous submissions cited there]). This relaxation is particularly needed in those cases in which only one community-based TLD application is involved. ICANN still proposes to treat these cases in the same way as those in which more than one applicant within a contention set claims the backing of a community. This seems unjustified.

VI. Module 5: Explanatory Memorandum: Thick v. Thin Whois for new gTLDs

IPC commends ICANN for modifying its proposal for new gTLD registry agreements to require "thick" Whois registries in response to the concerns of the Implementation Recommendations Team (IRT) and other commenters. As stated in several previous comments on the Draft Applicant Guidebook (DAG), IPC believes that provisions in the previous draft of the base contract regarding display of registrant contact information (via Whois) were too weak. A thick Whois at the registry level will provide greater transparency and accountability, as well as stronger protections against abusive registrations post-launch. As a result of the proposed shift in policy to thick Whois, copyright and trademark owners, as well as law enforcement, consumers, and members of the public, will have ready access to a full set of Whois data publicly available on each registration in the new gTLDs. Such information will help enable them to track down sources of, and further investigate and resolve, intellectual property infringements and other illegal or malicious conduct more expeditiously. This proposed change to thick Whois will strengthen the fight against online infringement of intellectual property, cybersquatting, phishing, pharming, malware, and other fraudulent or criminal acts . Further, it is consistent with the practice of the vast majority of existing gTLD registries. IPC welcomes these benefits of enhanced accessibility and increased stability, and believes that any privacy concerns are adequately addressed by existing procedures.

ICANN should also take this opportunity to provide incentives for the new registries to take on some of the responsibility for ensuring that the ICANN-accredited registrars which they employ to sponsor registrations live up to their obligations with regard to Whois. See discussion above in section II(D) of these comments.

Respectfully submitted,

GNSO Intellectual Property Constituency