MAY 14, 2010 ICANN DRAFT ADVISORY

ANALYSIS AND COMMENTS

I. Background:

On May 14, 2010, ICANN issued a three-page *[Draft] Advisory re: Registrar Accreditation Agreement Subsection 3.7.7.3* (hereinafter "Advisory")[1]. The Advisory's "Summary and Purpose" states its purpose is to clarify that:

(i) if a Registered Name Holder licenses the use of a domain name to a third party, that third party is a licensee, and is not the Registered Name Holder of record; and

(ii) the Registered Name Holder licensing the use of a domain name is liable for harm caused by the wrongful use of the domain name unless the Registered Name Holder *promptly identifies* the licensee to a party providing the Registered Name Holder with *reasonable evidence* of actionable harm. *(Emphasis added.)*

The net effect of the Advisory would render both Registrars and their privacy/proxy services (hereinafter collectively, "privacy services") liable for harm caused by the wrongful use of a domain name utilizing such privacy services, unless the privacy service promptly identifies the licensee when presented with reasonable evidence of actionable harm.[2]

II. ICANN Should Forgo the Advisory and Draft a New Provision that Addresses the Role of Privacy Services as Registered Name Holders.

For several years, ICANN has been concerned with privacy services' compliance with Section 3.7.7.3; specifically, that certain privacy services have repeatedly failed to disclose the identity of the Registered Name Holder when confronted with evidence of cyber squatting, intellectual property infringement, and other wrong-doing. To stem the tide of such irresponsible behavior, ICANN believes it must clarify that liability under Section 3.7.7.3 is properly imposed on non-compliant (i.e., non-enforcing) privacy services.

We note at the outset that Section 3.7.7.3 was drafted before privacy services

---

[1] http://www.icann.org/en/announcements/announcement-14may10-en.htm

[2] It has always been DBP's position that it is not subject to Section 3.7.7.3. DBP is an independent legal entity, and not a Registrar subject to ICANN oversight. Nor does it "license" the use of domains but instead, per the express terms of a legal agreement, holds them in "proxy" (i.e., as a substitute or agent of the customer). We will however, for purposes of this discussion (and without conceding our position) assume that the Advisory applies to DBP.

even arose – therefore, its continued application to privacy services and the proposed modifications set forth within the Advisory are akin to "fitting a square peg into a round hole." Moreover, the Advisory's proposed tinkering does not address the current situation of holding privacy services absolutely liable for wrongful use of a domain name over which they exercised no control.

We respectfully submit that ICANN should cease further work on the Advisory and instead proceed with its own Policy Development Process. That process would afford all affected entities an opportunity to sit at the table and contribute towards the crafting of a comprehensive Issues Report that expressly addresses those unique situations when the Registered Name Holder is a privacy service.

III. In the Alternative, Key Terms in the Advisory Should be Defined, and Certain Comments Eliminated.

If ICANN is not at the juncture where it is willing to draft a wholly new provision, then in the alternative we respectfully submit that the Advisory does not go far enough in its treatment of several critical issues, particularly the definitions of "prompt identification", "reasonable evidence", and "wrongful misuse." A failure to more clearly define these key concepts will render the existing Advisory a mere band-aid that does not adequately address ICANN's legitimate concerns with rogue privacy services; nor will it balance the rights of the intellectual property community and reputable privacy services, or protect the identity of privacy service customers facing meritless accusations.

Set forth below is a discussion of those areas of the Advisory that we contend are deficient, as well as proposed alternative language that would better serve the interests of all involved.

a. <u>The definition of "prompt identification</u>"

The Advisory pointedly acknowledges that, "[e]xactly what constitutes … 'prompt' identification is not specified in the RAA, and might vary depending on the circumstances." Moreover, it clearly contemplates that courts and arbitrators shall ultimately determine whether identification of a licensee is "prompt".

Absent a clear definition of the term "prompt", courts and arbitration panels are free to exercise an overly broad range of discretion that leaves privacy services dangling at their whim. If the Advisory neglects to articulate clear operational standards that can be implemented by privacy services, then we can be sadly confident in the knowledge that conflicting interpretations will be forthcoming. What one court or arbitration panel considers 'prompt identification' in one instance will surely be deemed inadequate by another.

We acknowledge that the Advisory indicates that any delay in excess of 5 business days might not be considered 'prompt'. But since the Advisory only speaks in

terms of "guidance", it leaves the door wide open for every court and arbitration panel ruling on a Section 3.7.7.3 issue to readily disregard such "guidance." As a result, the Internet community will be left to sort through a mishmash of inter-pretations regarding "prompt identification".

Moreover, the Advisory's failure to articulate a clear standard as to "business days" leaves open the door to court and arbitrator caprice to impose a "calendar days" standard – again potentially leaving the Internet community floundering in the wake of conflicting decisions. Further compounding the problem is the fact that all countries do not have the same business days; and many countries and businesses often close down for an entire week (if not longer) in observance of a national holiday. Unfortunately, "5" days will oftentimes be insufficient despite everyone's best intentions.

Confusion and non-uniformity will continue to be the order of the day and the Advisory, though well-intentioned, will not affect any real change. Imparting broad discretion to courts and arbitration panels guarantees that rogue privacy services will continue to have numerous opportunities to escape the imposition of liability. Yet those privacy services that take their obligations to the Internet and intellectual property communities seriously will continue to be on the receiving end of disparate decisions that unfairly foist liability upon them.

We submit that if the Advisory intends to clarify liability, it should seize the opportunity to specify that "prompt identification" is when the Registered Name Holder discloses the licensee's identity within 10 calendar days upon receipt of reasonable evidence of actionable harm from a party.[3]

Another example of the Advisory's grant of excessive discernment to courts and arbitration panels is found in the following statement: "It would ultimately be up to a court or arbitrator to assess and apportion liability in light of the promptness of a Registered Name Holder's identification of a licensee." This statement raises the distinct possibility *that even if a privacy service disclosed the licensee's identity on the 5th business day, a court or panel could still rule that it should have disclosed prior to that date – and then hold the privacy service liable.*

We further submit that the Advisory must eliminate this commentary in order to thwart the unjust imposition of liability onto compliant privacy services.

b. The definition of "reasonable evidence of actionable harm"

Similar to "prompt identification" the Advisory states, "[e]xactly what constitutes 'reasonable evidence of actionable harm' … is not specified in the RAA, and might vary depending on the circumstances." The absence of a well-articulated definition

[3] We similarly take issue with the phrase "reasonable evidence of actionable harm" and discuss an alternative standard infra.

for "reasonable evidence" leaves privacy services even more rudderless than the absence of a clear directive for "prompt identification."

A fundamental precept of due process is that anyone subject to potential liability deserves notice as to the circumstances that precipitate such liability. Otherwise, one cannot conform their behavior accordingly. Yet here, privacy services have no idea as to what will (or will not) constitute "reasonable evidence" and thus have no basis upon which to act (or not act). The presentation of certain evidence which one forum deems inadequate (thus leaving the non-disclosing privacy service vindicated), will almost certainly be deemed adequate in another forum – thus leaving the non-disclosing privacy service accountable.

Granted, the Advisory attempts to address this ambiguity, noting with respect to intellectual property infringement claims that, "documentation of ownership of a trademark or copyright, along with documentation showing alleged infringement, *should generally* constitute reasonable evidence of actionable harm." *(Emphasis added.)* But the open-ended standard of "should generally" leaves it susceptible to the subjectivity of courts and arbitration panels. It is wholly conceivable that a privacy service that refuses to disclose the licensee's identity based upon an absence of documented trademark ownership could still be found liable.

As if this were not confusing enough, the Advisory posits – again by way of "guidance" – that "'reasonable evidence of actionable harm' does not imply a requirement of the filing of a formal process (such as a UDRP complaint, civil lawsuit or the issuance of a subpoena), but again it will be up to a court or arbitrator to decide whether the evidence constitutes "reasonable" evidence." It is unclear as to what direction privacy services are to glean from such a statement - perhaps that they can disregard the filing of a formal process? Conversely, if the filing of a formal legal process can subsequently be deemed by a court or arbitrator as "insufficient", then with what certainty can privacy services act when they are served with such notice?[4]

[4] Finally, the Advisory states that "...with respect to claims of intellectual property infringement, documentation of ownership of a trademark or copyright, along with the documentation showing alleged infringement, should generally constitute reasonable evidence of actionable harm." DBP submits that the possibility always exists that a set of unique circumstances will arise that do not permit a complaining party to provide documentation of both trademark ownership and infringement. Privacy services should not be compelled to operate under absolute constraints, but rather, should have the *option* of considering such documentation, together with "other relevant evidence of trademark infringement under the totality of the circumstances." Doing so prevents privacy services from having to make judgment calls as to the legitimacy of trademark documentation issued by different countries, and also provides redress for intellectual property holders with legitimate claims who, for defendable reasons, are unable to comply with strict document production requirements.

Ultimately, and for all of the reasons articulated above, the Advisory falls short of providing any concrete guidance upon which courts, arbitration panels and privacy services can confidently rely.

We submit that the Advisory should adopt the institution of a formal legal process as its "reasonable evidence" standard. Specifically, "reasonable evidence" would exist if the privacy service receives notice that a domain name utilizing its service is named as a Respondent in: (i) a UDRP proceeding, or (ii) a lawsuit in a court of competent jurisdiction. There are several strong justifications for doing so.

First, the institution of such proceedings requires the Complainant to pay filing fees upfront, which by their very nature goes a long way towards eliminating frivolous claims against privacy service customers.

Second, such a benchmark would eliminate the burden borne by privacy services in having to decipher trademark ownership documentation issued by different countries, and in making determinations as to whether infringement and/or cyber squatting has occurred. Compelling privacy services to disclose only when confronted with formal legal proceedings eliminates the "guesswork" by the privacy service, as well as conflicting determinations by courts and arbitrators as to whether "reasonable evidence" has been presented in any given instance.[5]

Third, requiring commencement of either a UDRP proceeding or lawsuit as the applicable standard is not a foreign concept, and in fact, mirrors a UDRP requirement with which all Registrars are familiar. Section 3 of the UDRP ("Cancellations, Transfers and Changes") provides that Registrars may only cancel, transfer or make changes to a domain name upon receipt of: (i) instructions from the customer; (ii) an order from a court or arbitral tribunal requiring such action; or (iii) a decision from an Administrative Panel requiring action in a UDRP proceeding.

If Registrars' impetus to act is an order from a court or arbitral tribunal then it is logical to extend this same standard to privacy services. That is, privacy services' impetus to disclose would be upon receiving notice about the institution of a formal legal process. Embracing such a standard would not radically alter the playing field that currently exists.

We further submit that the Advisory should take the initiative in addressing the concerns of law enforcement organizations worldwide, and clearly mandate that privacy services are equally responsible for disclosing the licensee's identity when contacted by law enforcement about an investigation into the "wrongful use of a

[5] The purpose of the Advisory (presumably) is to clearly promulgate the minimum standards with which *all* privacy services must comply. Yet those privacy services at the forefront of the industry (and which have plenteous staffing and legal resources) would be free to adopt a more liberal disclosure policy. For example, such privacy services could disclose a licensee's identity when presented with evidence of trademark infringement by a law firm representing a well-known trademark holder prior to the commencement of a formal proceeding under the UDRP.

domain name."

Finally, the Advisory's modification of Section 3.7.7.3 should not proceed in a vacuum. Concurrent with the adoption of the standard suggested herein, now would be an opportune time for ICANN to amend the UDRP in conjunction with any changes to Section 3.7.7.3 so that an arbitration proceeding can only proceed against the disclosed licensee and not the privacy service.

The UDRP Rules currently state that, "Respondent means the holder of a domain-name registration against which a complaint is initiated." Similar to Section 3.7.7.3, this definition does not encompass the existence of privacy services, as it was drafted prior to the arrival of such services in the Internet arena. As a result, arbitration panels are continuously compelled to determine the proper Respondent on a case-by-case basis -- sometimes finding it is the "licensee", the privacy service, or both.

We suggest that even if ICANN is not predisposed to revising the definition of "Respondent" it could, at a minimum, require that upon receiving information as to the licensee's identity and contact information, Complainants must amend their pleadings to name the licensee as Respondent while concomitantly removing the privacy service.[6]

c. The definition of "wrongful use"

Notably, the Advisory does not take the opportunity to further define Section 3.7.7.3's phrase, "wrongful use of the domain"; nor does it provide any guidance as to its interpretation. We submit that if the Advisory is going to address the concepts of "prompt" and "reasonable evidence" then it cannot ignore "wrongful use." Not only will such a definition provide sorely needed guidance, but more importantly, it removes another justification upon which so many rogue privacy services rely in failing to act. That is, such services wholly fail to disclose because there is no indication as to what constitutes "wrongful use." But with an articulated standard for "wrongful use" together with the more substantive standards discussed supra, ICANN could confidently move against those ineffectual privacy services who continue to be non-compliant.

We therefore suggest that the Advisory define "wrongful use" to include those situations when the domain name: (i) violates or infringes a third party's trade-mark, trade name or other legal rights; (ii) is engaged in illegal activities such as terrorism, hate crimes, child pornography or drug trafficking; (iii) is engaged

[6] This would accomplish the following: (i) eliminate the time expended by arbitration panels in issuing decisions that discuss the privacy service's relationship to the licensee *ad nauseam*; (ii) expedite the processing of arbitration claims; (iii) promote the legitimate right of the licensee (and not the privacy service) to mount a defense regarding the domain name; (iv) and, in the case of non-disclosing or rogue privacy services, allow arbitration panels to properly impose liability on those that are not responsible members of the Internet community.

in the transmission of Spam, viruses, Trojan Horses, backdoors, worms, time-bombs or any other code, routine, mechanism device or item that corrupts, damages, impairs, interferes with, intercepts or misappropriates software, hardware, firmware, network, system, data or personally identifiable information; (iv) is involved in phishing; (v) is defamatory, abusive, or threatening; (iv) violates state or federal laws, or any other applicable law, of a sovereign country, provided that the Registered Name Holder is subject to the jurisdiction of that country.[7]

IV. Summary and Proposed Alternative Language

In summary, we respectfully recommend that ICANN take the following steps with respect to the Advisory:

1. Suspend further action on the Advisory and proceed with its own Policy Development Process so as to permit affected entities the opportunity to collectively draft a comprehensive Issues Report that expressly addresses the situation when a Registered Name Holder is a privacy service.

2. In the alternative, proceed with its intended clarifications as articulated in the Advisory's "Summary and Purpose" (see page 1, supra), but eliminate all statements allowing courts and arbitrators to:

    - rule on issues of "prompt identification" and "reasonable evidence of actionable harm."

    - assess and apportion liability in light of the Registered Name Holders' "promptness" in identifying a licensee.

3. Further revise Section 3.7.7.3 to specify:

    - a time period of 10 calendar days for Registered Name Holders to disclose a licensee's identity (as opposed to a standard of "prompt identification").

    - that Registered Name Holders shall be held liable in the event they fail to disclose a licensee's identity when presented with notification of a formal legal process (as opposed to being presented with "reasonable evidence").

    - the conduct that will constitute "wrongful use" of a domain name.

[7] Such language would hopefully discourage forum-shopping.

4. Amend the UDRP so that upon disclosure of the licensee's identity, the arbitration proceeding can only proceed against the disclosed licensee and not the privacy service.

To assist with ICANN's implementation of the aforementioned recommendations, we propose the following alternative (and highlighted) language for Section 3.7.7.3:

> Any Registered Name Holder that intends to license use of a domain name to a third party is nonetheless the Registered Name Holder of record and is responsible for providing its own full contact information and for providing and updating accurate technical and administrative contact information adequate to facilitate timely resolution of any problems that arise in connection with the Registered Name. A Registered Name Holder licensing use of a domain according to this provision is liable for harm caused by wrongful use of the domain, *unless* it discloses both the identity of the licensee and the contact information provided by the licensee within ten (10) calendar days of receiving a clear, written notification that the licensee is
>
> (a) named as a Respondent in either a UDRP proceeding or a lawsuit filed in a court of competent jurisdiction; or
>
> (b) the subject of an investigation by a law enforcement organization.
>
> The Registered Name Holders' disclosure obligation shall be to the party providing the written notification.
>
> For purposes of this Section 3.7.7.3, the term "wrongful use" shall Include those situations when the domain name, and/or the content associated with it:
>
> (i) violates or infringes a third party's trademark, trade name or other legal rights;
> (ii) is engaged in illegal activities such as terrorism, hate crimes, child pornography or drug trafficking;
> (iii) is engaged in the transmission of Spam, viruses, Trojan Horses, backdoors, worms, time bombs or any other code, routine, mechanism device or item that corrupts, damages, impairs, interferes with, intercepts or misappropriates software, hardware, firmware, network, system, data or personally identifiable information;
> (iv) is involved in phishing;
> (v) is defamatory, abusive, or threatening;
> (iv) violates the state or federal laws, or any other applicable law, of a sovereign country, provided that the Registered Name

Holder is subject to the jurisdiction of that country.

For purposes of this Section 3.7.7.3, the requirement of a "clear, written notification" shall be deemed satisfied when it identifies:

(i) the complete name of the arbitral forum or court where the proceeding has been commenced;
(ii) the date when the proceeding was filed;
(iii) the domain name(s) that are at issue in the proceeding;
(iv) the party or parties commencing the proceeding together with their complete contact information (including name, phone number, email, and postal address).

Email communications shall constitute acceptable written notification to the Registered Name Holder.

Finally, we appreciate the opportunity to provide our thoughts as to the Advisory and welcome any additional opportunities to be part of the drafting process.

Nima Kelly
Vice President, Domains By Proxy, Inc.