January 15, 2007

Comments on the *Preliminary Task Force Report on Whois Services*

On behalf of the companies and organizations listed below, we write to provide our comments on key aspects of the Operational Point of Contact ("OPoC") and Special Circumstances Proposals contained in the *Preliminary Task Force Report on Whois Services*, and on the proposals for access to Whois data that are summarized on pages 24-27 of the *Preliminary Task Force Report on Whois Services.* As discussed further below, we have significant concerns about and objections to the OPoC proposal. We believe the Special Circumstances proposal strikes a better balance between addressing registered name holder ("RNH") privacy concerns while preserving the critical ability to access RNH contact data in a timely manner. We also have concerns about and objections to many of the informal proposals for access to data no longer disclosed in Whois that are contained in pages 24-27 of the *Preliminary Task Force Report*.

OPoC Proposal

The OPoC proposal would eliminate from published Whois data the RNH's postal address, city, and postal code, and would eliminate all information – most notably the telephone number, fax number, and email address – for the administrative and technical contacts (collectively, the "RNH contact data"). Only the RNH's name, state/province, and country will remain publicly accessible. In most instances, it will be exceedingly difficult if not impossible to locate an individual RNH based solely on that accessible information. Detailed contact information will be accessible only for the person or entity designated by the RNH as its OPoC. Under the current proposal, the OPoC has no obligation to forward to the RNH any communications of any kind other than those directly related to resolving operational issues. Further, the OPoC proposal contains no "minimum qualification" requirements or standards for the OPoC. Similarly absent is a requirement that the OPoC provide advance consent to being so designated. Consequently, an individual RNH could designate his neighbor or former employer as the OPoC and the designee would not learn of its designation until a problem arose.

The OPoC proposal will cause significant delays in accessing critical RNH contact data and may well effectively eliminate that access. Such delays and elimination could cause harm to consumers, including the very consumers that the OPoC proposal is ostensibly intended to protect. The OPoC proposal raises serious questions as to where (and how) a person with a legitimate interest in accessing the RNH's contact data could pursue that access and whether a U.S. court would ever grant it. In addition, the OPoC proposal calls into question the ability of owners of U.S. trademarks and service marks to pursue in rem causes of action under the U.S. AntiCybersquatting Consumer Protection Act. 15 U.S.C. § 1125(d) et seq.. In both circumstances, the RNH itself – the very person the OPoC proposal is ostensibly designed to protect – could be deprived of notice and the opportunity to be heard. We elaborate on each point below.

On its face, the OPoC proposal will cause significant delays in accessing critical RNH contact data – postal and email addresses, and telephone numbers – and may well effectively eliminate that access. Immediate access to such RNH contact data is critical for

companies such as ours because it is essential to our ability to act promptly against cybersquatters, to stop quickly the online sale of counterfeit products, and/or to counteract immediately phishing schemes or other online fraud schemes. (We note that the OPoC proposal is also devoid of any provision for providing law enforcement authorities with access to this RNH contact data.) The longer a phishing scheme operates in association with a particular domain name, the greater the number of consumers who will be harmed financially and the greater the severity of that harm. Similarly, the longer counterfeit products can be sold and offered for sale through a website associated with a particular domain name, the greater the number of consumers who will be harmed. This is especially true for any counterfeit products capable of causing physical harm. Finally, the longer a cybersquatter can use an infringing domain name, the greater the number of consumers who are likely to be harmed by consumer confusion. Delays of even one day can, and do, entail significant consequences.

It has been suggested that the OPoC proposal, once implemented, would coexist with private registration services. The overlay of private registration on top of OPoC would further exacerbate the delays and inaccessibility noted above.

The OPoC proposal also raises serious questions as to where (and how) a person with a legitimate interest in accessing the RNH's excluded contact data could pursue that access, whether any U.S. court would grant such access, and how the RNH would receive notification of the proceeding. We assume for purposes of illustration that the underlying claim (e.g., infringement, cybersquatting, counterfeiting, phishing) would be within the subject matter jurisdiction of a U.S. federal court and that both the registrar and RNH are domiciled in the United States.

At a minimum, the OPoC proposal raises the following questions: In which federal district court would a party pursue access? The U.S. District Court for the Central District of California, where ICANN is located? The federal district in which the registrar is located? The federal district in which the ISP hosting the associated website (assuming there is one) is located? The federal district where the RNH is located? For those 24 states that contain more than one federal district, would the most populous district be considered the "default" district?

Independent of the forum issue, how does one provide the RNH with service of process for the purpose of providing notice? The name, state/province, and country information in the Whois record does not provide sufficient detail to permit service and the OPoC has no obligation to forward such communications or to accept service. Will it be necessary for the party seeking access to the RNH contact data to have the court issue a subpoena to ICANN? To the registry? To the registrar?

Even if a court were to allow the matter to proceed without service, it seems unlikely that, for example, the U.S. District Court for the Southern District of New York would entertain an action where the only basis for personal jurisdiction over the registered name holder-defendant were (i) the fact that Whois identified the RNH's state as New York; and (ii) the fact that the district is the most populous one in the state.

With regard to specific actions, the OPoC proposal could prevent the owners of U.S. trademarks or service marks from using the principal method for obtaining in rem jurisdiction under the U.S. AntiCybersquatting Consumer Protection Act ("ACPA"), 15 U.S.C. § 1125(d) et seq, and could, in light of the issues noted above, potentially preclude all claims under ACPA. ACPA provides for two causes of action – in rem against the domain name itself and in personam against the domain name registrant/registered name holder. In light of the difficulties noted above, most owners of U.S. marks may have no alternative but to seek to proceed in rem instead of in personam.

Under ACPA, a mark owner usually obtains in rem jurisdiction by showing that it was not able to find a person who would have been a defendant even though the owner exercised due diligence by "sending a notice of the alleged violation and intent to proceed under this paragraph to the registrant of the domain name at the post and e-mail address provided by the registrant to the registrar; and publishing notice of the action as the court may direct promptly after filing the action." 15 U.S.C. § 1125(d)(2)(A)(ii)(II). The trademark owner obviously cannot send any such notice of alleged violation to the RNH's post and e-mail addresses if the owner does not have access to those addresses. The OPoC proposal excludes those addresses from the published Whois data.

The other method for obtaining in rem jurisdiction under ACPA is to persuade the court to find that the owner "is not able to obtain in personam jurisdiction over a person who would have been a defendant in a civil action under [§ 1125(d)(1)]." Courts could potentially make such a finding based solely on the trademark owner's recitation of the inability to access RNH contact data sufficient to establish personal jurisdiction anywhere. The mark owner would then proceed in rem, which might effectively deprive the RNH of notice and the opportunity to be heard.

Alternatively, courts might find that the trademark owner had not met its burden of showing an inability to obtain in personam jurisdiction and, as a result, refuse to allow the owner to proceed in rem. Under such circumstances, the trademark owner could not proceed under ACPA either in personam or in rem.

Finally, we also have some concern about the portion of the OPoC proposal relating to complaints about inaccurate Whois data. The proposed "remedy" for an RNH's failure to update or correct the alleged inaccurate Whois data is to place the domain name on "hold." Regardless of whether placing a domain name on "hold" means either that the name will continue to resolve but no changes can be made to the registration or that the name will not resolve and no changes can be made to the registration, this "remedy" is insufficient. Because complaints about Whois data accuracy are most likely to arise when the domain name is being used in a way objectionable to the complaining party, allowing the domain name to continue to resolve perpetuates the objectionable use. Similarly, permitting the RNH to maintain the registration despite its willful failure to correct or update its Whois data also perpetuates the objectionable conduct.

For these reasons, we encourage rejection of the current OPoC proposal.

Special Circumstances Proposal

We believe that the Special Circumstances proposal strikes a better balance between privacy concerns while preserving the critical ability to access RNH contact data in a timely manner. Its eligibility requirements are sufficiently tailored to protect from disclosure the contact information for those individuals whose personal safety or security would be jeopardized while limiting through the proposed non-commercial use requirement and numerical ceilings the number of domain names for which RNH contact data would be shielded. Requiring periodic monitoring of the domain name's use will also minimize the abuse of the disclosure shield. Further, the inclusion of a challenge mechanism that would be available to the potential applicant, law enforcement, and others with a legitimate objection to the designation also ensures both that eligible individuals are not rejected and that the Special Circumstances designation is not used for illegitimate purposes.

Other Proposals for Access to Data Removed from or Shielded from Whois

We comment below on each of the proposals for access to data no longer disclosed in Whois that are contained in pages 24-27 of the *Preliminary Task Force Report.*

1. Obtain Contact Data From Registrar. A proposal that parties seek to obtain RNH contact data from the registrar and that the registrar disclose the RNH contact data to a requesting party is not only unworkable but will undoubtedly impose significant business costs on both the requesting party and the registrar. First, it is highly doubtful that any registrar could provide the RNH contact data in the short timeframe that we believe is essential. Immediate turnaround seems unlikely. Second, the disclosure of the RNH contact data should not be within the discretion of the registrar. Third, the proposal could result in extensive litigation that would unduly tax the resources of the registrar, the requesting party, and the courts. It is in no one's interest to adopt a proposal that could potentially result in an incessant stream of court actions in which the registrar was either named as a defendant and subject to discovery or named as a third party and subject to subpoena.

2. UDRP Mechanism. The substance of the proposal is not clear from the report. Accordingly, we reserve comment at this time.

3. Process for Disclosing Access to Whois Data. We have concerns about the ability to use the proposed process in the short timeframe we believe is essential. Immediate determinations of whether access will be granted and disclosure of the withheld data, which are critical in instances of online fraud, online counterfeiting and cybersquatting, seems unlikely. We reserve comment on any future elaboration of the requesting process, standards for disclosure, and identification and qualification of the third party selected to make the determinations.

4. Contractual Limitations on Use of Data. Because there is no real detail as to the contractual specifications and technical mechanism contemplated by such a proposal, we reserve comment.

5. Domain Name Lapse In Lieu of Disclosure. We object to this proposal because preventing the domain name from resolving in the future does not "cure" the past harm caused by a "phisher", a company selling counterfeit products online, a cybersquatter or perpetrator of other online fraud. Access to the RNH contact data remains essential.

* * *

Thank you for your consideration of these comments.

Respectfully submitted,

American Standard Inc.
Bank of America Corporation
Belo Corp.
Expedia, Inc.
First California Mortgage Company
International Federation of Film Producers Associations
International Video Federation
Marina District Development Company, LLC d/b/a Borgata Hotel Casino & Spa
The MCPS-PRS Alliance Limited
M Financial Holdings Incorporated
National Geographic Society
The Procter & Gamble Company