International Trademark Association
Representing the Trademark Community since 1878

Via Electronic Mail

January 15, 2007

Comments of the Whois Subcommittee of the International Trademark Association on the GNSO Whois Task Force Preliminary Task Force Report on Whois Services

RECOMMENDATION

The Whois Subcommittee of the International Trademark Association (INTA) recommends that the GNSO Council adopt a modified version of the Special Circumstances model for Whois access, consider emerging proposals to prevent abuse of the Whois through technical and contractual means, and reject entirely the Operational Point of Contact (OPoC) model.

SUMMARY OF COMMENTS

If ICANN adopts any change to the current Whois system, a modified Special Circumstances model would best serve the needs of brand owners and users, as well as the general public.

The Special Circumstances model offers the following clear advantages over the OPoC Model:

- it properly balances the need to facilitate the resolution of legal disputes with the rare instances where there is an urgent, legitimate need for a registration to be maintained anonymously
- it drastically diminishes the abusive use of current proxy registration schemes
- it facilitates communication with registrants concerning violations of law and the provision of legal notice upon registrants

By contrast, the OPoC model is riven by weaknesses, including:

- the lack of a requirement that OPoC pass on communications other than operational, technical communications, such as legal demands, and legally required notices,
- the lack of agreement by the registrant that providing such notice to the OPoC is equivalent to providing it to the registrant
- the lack of any standards for the timely transmission of communications
- the lack of any means of enforcing that the OPoC fulfills its obligations

Finally, this comment briefly discusses other proposals offered since the report's publication.

ABOUT INTA AND THE WHOIS SUBCOMMITTEE

INTA is a 128-year-old global organization with members in 180 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 also served as the leading voice of trademark owners in the development of cyberspace, including as a founding member of ICANN's Intellectual Property Constituency. INTA's Whois Subcommittee is a group of over twenty trademark attorneys and professionals charged with monitoring adoption or modification of Whois policies in new and existing TLDs and advocating for adequate access to domain ownership information.

INTA has a particular interest in policy relating to the Whois database, because the information contained in the Whois database assists trademark owners and authorities in policing abuses of intellectual property and preventing consumer confusion and consumer fraud. Moreover, the information in Whois also allows Internet users and consumers from all walks of life to identify the owners of web sites selling goods or disseminating information over the World Wide Web.

PURPOSE OF WHOIS ACCESS

On April 12, 2006, the GNSO Council recommended a preliminary, working definition of the purpose of the gTLD Whois service:

> "The purpose of the gTLD Whois service is to provide information sufficient to contact a responsible party for a particular gTLD domain name who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name with a DNS name server."[1]

The Whois database is the primary means for consumers to identify site operators with whom they do business, or who use domains to perpetrate fraud. Whois is also the primary means for brand owners to identify parties responsible for online infringement—imitations that result in consumer confusion. To ignore these legitimate and important uses of Whois, which have been common since the dawn of commercial activity on the Internet, and as a result to curtail access to domain registration information, would greatly inhibit the operation of law on the Internet. Therefore, we respectfully reiterate our comments on the purpose of Whois,[2] and urge the GNSO to revise its definition of the purpose of Whois.

STRENGTHS OF THE SPECIAL CIRCUMSTANCES MODEL

Registering an Internet domain means acquiring a property that is both unique and, given the global and globally accessible nature of the Internet, usually intended to be used in an open or public fashion. Thus, owning a domain should be treated like other property acquisitions—for example, owning real estate, registering a trademark, or establishing the right to do business

[1] http://gnso.icann.org/issues/whois-privacy/
[2] Available at http://forum.icann.org/lists/whois-comments/msg00025.html.

under a fictitious name. In other words, domains ownership information should, generally, be available publicly for the security of the public, and the regular adjudication of legal rights.

A. The Special Circumstances System Strikes the Right Balance

The Special Circumstances model serves the public interest in consumer protection and the protection of legitimate trademark rights best because it adheres to two basic principles:

(1) The Special Circumstances proposal properly treats domain registrations and the operation of web sites as essentially public acts, and
(2) The Special Circumstances proposal addresses legitimate concerns that militate for the privacy of some domains to protect those with legitimate, urgent reasons for protection.

Importantly, trademark owners are not the only vulnerable parties. The security of the general public is an equal interest, which the Special Circumstances model serves. If a registrant uses a domain name for commercial purposes, consumers should be permitted easy access to registrant information at little or no cost in order to verify their legitimacy or contact registrants, such as where a product purchased from a registrant turns out to be faulty. Further, easy access to registrant information for trademark owners also assists in consumer protection, as trademark owners can track down and take appropriate action against misuse of their properties which may be misleading or confusing consumers.

B. The Special Circumstances System Replaces Proxy Registration Systems

Simply, the Special Circumstances model eliminates proxy registrations from the Whois database. Under the Special Circumstances model, all listed registrants would, as under the current system, be deemed the legal owners of domains. This provides certainty in determining what party owns a domain, both for holding site owners accountable for violating the law, and for other purposes, such as in transactions for the transfer of domains as corporate assets.

C. Special Circumstances Protects those with Real, Concrete Needs to Protect their Identities

The Special Circumstances model strikes the right balance between protecting those with legitimate, urgent needs for anonymity, and maintaining public accountability for the ownership of domain names. Exemptions from full public disclosure would be limited only to individuals who could demonstrate that public display of their contact information or identity will "jeopardize a concrete and real interest in their personal safety or security that cannot be protected other than by suppressing that public access."

D. Reliability Lowers Net Costs and Improves Utility

The greater openness of access to Whois information under the Special Circumstances model would reduce the costs involved with enforcing legal rights. Without a mask for registrants to hide behind, a party seeking to enforce its rights need not undertake multiple rounds of litigation, first to remove the mask, and then pursue claims against a domain registrant, who might be in a

different jurisdiction. This reduces the time and effort involved in enforcing rights, and promotes swift and meaningful redress of legal wrongs.

The greater openness of access to Whois information under the Special Circumstances model would greatly improve efficiency of investigations and increase the value of their results in comparison to the current "proxy" services or the proposed OPoC model.

E. Additions to the Special Circumstances Proposal

a. Cost Could be Allocated to Registrants and Information-Seekers

The Special Circumstances proposal (paragraph 4) calls for payment out of "existing volume-sensitive (i.e., per registration transaction) fees currently paid by registrars and/or registries." We believe it may be worth considering whether to fund the system (or augment funding of the system) through nominal fees upon registrants applying for special-circumstances status, just as registrants pay extra for proxy registrations currently.

a. The Special Circumstances System Should Be Reevaluated Periodically

Because of the cost and infrastructure required by the Special Circumstances system, we suggest that the system include a sunset provision, so that retaining the system is conditioned upon a determination that the need of Special Circumstances applicants to protect their identities justifies the cost. The use of narrow, tailored criteria for a registrant to protect his data would create easy test cases to monitor the effectiveness of the model in both (1) protecting truly vulnerable registrants and (2) minimizing the costs to operate the model.

DEFICIENCIES OF THE OPoC MODEL

In their zeal to protect the privacy of domain name holders, the drafters of the OPoC model have proposed a more effective screen for wrong-doers than even the proxy registrations allowed under the current Whois system. If a third-party contact is to substitute effectively for the ability to locate and identify the actual owner of a domain, that contact must have specific responsibilities for passing communications—up to and including service of legal process—on to the domain name holder. Further, those responsibilities must be enforceable. Yet, the OPoC proposal provides neither of these things. Moreover, OPoC would weaken the utility of the UDRP, making resolution of domain disputes more costly.

A. The OPoC Proposal Fails to Make the OPoC Responsible for Reliably Passing Communications on to Domain Name Owners

In specifying the responsibilities of the OPoC, the proposal states only, "The purpose of the operational point of contact is to resolve, or to reliably pass on data to resolve, operational issues relating to a domain name. At a minimum, this must include the resolution of issues relating to the configuration of the records associated with the domain name within a DNS nameserver." The OPoC proposal fails to ensure that data are reliably passed on to domain name owners. Domain name owners and third parties must be confident that important communications

pertaining to a domain name have been effectively communicated to those with legal responsibility for resolving issues about domain ownership and use. The system should also include the registrant's agreement (likely contained in the registration agreement with the registrar) that if the registrant appoints an OPoC, providing such notice to the OPoC is equivalent to providing it to the registrant.

1. The OPoC Proposal Limits Contact with Domain Name Owners to "Operational" Issues

The OPoC proposal is unacceptably limited to an "operational" contact, only responsible for passing on data relating to "operational," *i.e.*, technical or administrative issues. For example, although the proposal allows registrants and OPoCs to agree voluntarily on additional responsibilities, the proposal would not require that the OPoC be able to pass on cease-and-desist demands, or the service of legal complaints or notices. Because contact information for the domain name holder would no longer be listed in the Whois, this could frustrate the ability of complainants to institute legal proceedings by providing legally-mandated notices, or to avoid the need for legal proceedings through informal contacts with the domain owner.

2. The OPoC Proposal Fails to Provide Reliable Standards for Timeliness or Guarantees of Delivery

In addition to the limited scope of communications the OPoC must pass on, the OPoC proposal includes no standards for how promptly communications must be passed on, or even verification that the communications have been delivered at all. A mechanism is not reliable if it is not timely. Law enforcement agencies and intellectual property owners who are entitled to the immediate take-down of an illegal web-site should not be forced to wait for indefinite periods of time before the domain name owner is notified. The fact that the OPoC model imposes no timetable for notifying "real" domain registrants that take-down proceedings are pending will create uncertainty and unnecessary delay, and risks leaving the public exposed to phishing schemes and other fraudulent conduct.

A mechanism is also unreliable if a third party cannot be assured that the domain name owner actually receives notices sent to him. The OPoC proposal does not guaranty that communications will ultimately be delivered to a responsible individual nor require any written confirmation of receipt. The onus is on the registered name holder to ensure he/she receives the data. Although the current system also puts responsibility for placing accurate information in the Whois on the name holder, the sender is able to determine if delivery has failed (such as because the postal service returns a letter as undeliverable or an e-mail "bounces"). Under OPoC, since the complaining party relies on the OPoC to forward the communication to the registrant, the complaining party may never know that its communication was not delivered.

B. The OPoC's Responsibilities are Not Enforceable

To be effective, a proposal must include provisions for its own enforcement. The OPoC Proposal contains no provision for penalizing an OPoC who fails to perform its duties, however limited those may be. On the contrary, the OPoC proposal insulates the OPoC from any such

responsibility by placing the burden upon the registered name holder to ensure that he receives the data. By comparison, under the current system, the party identified in the Whois is considered the owner-of-record of the domain name registration.[3] Thus, if the operator of a proxy service undertakes to place its own information in the Whois, the operator undertakes to act as a kind of trustee of the registration of the name, holding legal title to the domain for the benefit of the beneficial owner of the domain.[4] This, in turn, provides an incentive for a registrar or a proxy company to provide the name of the real party in interest where the ownership or use of the domain gives rise to legal liability. If the proxy service fails to divulge the beneficial owner's name, it risks being sued itself.[5]

This feature of the current system would disappear under the OPoC model. An OPoC would be neither the legal owner nor the agent for the legal owner. The OPoC would have no contractual relationship with the registrar (or, by extension, ICANN), but only with the registrant. Thus, ICANN would have no way to enforce the OPoC living up to its responsibilities, and no way to facilitate policing by the public (as ICANN forces registrants to agree to in the case of the UDRP). With the OPoC legally shielded from liability, and the registrant practically shielded from disclosure of its identity, the OPoC proposal would greatly reduce the accountability of the Internet's bad actors to the law.

COMMENTS ON ADDITIONAL PROPOSALS

There is a great chasm between the Special Circumstances proposal—which preserves easy access to domain registrant information for law enforcement and owners of legitimate intellectual property rights but only addresses the most life-threatening abuses of Whois data—and the OPoC proposal—which, in defense of vaguely-defined claims to "privacy" greatly endangers the practical enforcement of law on the Internet by throwing up great hurdles to access by legitimate rights owners and law enforcement. In this chasm, various Task Force members have suggested similar hybrid proposals that would, in their most basic elements, condition access to full Whois information on the searcher clearing technical security measures and/or contractually agreeing not to use the information for a list of specified improper uses (such as data mining for marketing purposes).[6]

---

[3] Registrar Accreditation Agreement, paragraph 3.3.1 (the Registered Name Holder is listed in the Whois).

[4] *E.g.*, Domains by Proxy provides that the domain will "be registered in the name of DBP, as Registrant" (http://www.securepaynet.net/gdshop/legal_agreements/show_doc.asp?pageid=domain_nameproxy&prog_id=domainsbyproxy).

[5] Of course, the current proxy system is far from ideal. Despite the theoretical risk of liability, in our experience, some proxy operators never respond to legal requests or confirm that communications have been passed on to the domain registrant. Proposals to regulate or reform the proxy system are beyond the scope of this comment.

[6] Examples of such proposals may be found in:

- Marilyn Cade, *Pragmatic and Achievable Steps toward Addressing Concerns about Public Access to WHOIS Services*, January 6, 2007, http://forum.icann.org/lists/gnso-dow123/msg01299.html (proposing: a. eliminating unrestricted port 43 Whois access in favor of web-based access—which might include click-though contractual terms of use, and b. allowing bulk access only to legitimate parties bound by contractual terms on the information's use); and
- Jordyn Buchanan, *Hybrid Tiered Access Proposal*, November 1, 2007, http://forum.icann.org/lists/gnso-dow123/msg01206.html (proposing that standard Whois output be changed per the OPoC proposal, but those who clear "a fairly low bar… everyone who agrees (by contract)" that "they will not use the data for various bad purposes (TBD)" get full access, while the rare case where disclosure would jeopardize a

While we are concerned over the complexity of a "tiered access" system, a simple requirement not to use Whois data for various bad purposes merits further discussion. For one thing, many large registrars already use image verification techniques and impose such contractual conditions, pursuant to paragraph 3.3.5 of the Registrar Accreditation Agreement.[7] Providing registrars a contractual cause of action against Whois abusers may give them an incentive to enforce Whois limitations, much the way the U.S. CAN-SPAM act has enabled successful suits by many large ISPs against high-volume spammers. Various issues, such as the list of prohibited uses, remain to be addressed. Moreover, any such system should preserve the ability for easy "one-stop" access to Whois information by consumers, which is currently served by registrars and third-party sites who display Whois results, even for domains they do not sponsor, through use of port 43 Whois. Nevertheless such proposals merit further discussion.

However, one proposal that should be rejected is the proposal completely to waive registrars' obligations to provide access to Whois information.[8] The proposal is founded on the premise that, "There are many other uses of gTLD Whois - most or all of which have been documented by the GNSO Whois Task Force. Creating policy to manage, influence, prevent or encourage most of this use is out of scope for ICANN." Quite simply, the idea that eliminating Whois is a policy-neutral action consistent with ICANN's technical mandate is a fallacy. As this comment makes clear, curtailing Whois would have a profound policy impact—by obstructing the means necessary to investigate and prevent violations of law. In fact, it is by maintaining a robust Whois that ICANN can, consistent with its core values, best defer to and facilitate the legitimate public policy role of governments and enhance the stability and security of the Internet as a medium for communications and commerce.

CONCLUSION

We thank the task force for the opportunity to provide these comments.

If there are any questions concerning this submission, please contact Bruce MacPherson at bmacpherson@inta.org.

"concrete and real interest in their personal safety or security" would entitle the registrant to complete removal, per the Special Circumstances proposal, absent legal process).

[7] *See, e.g.*, http://who.godaddy.com/whoischeck.aspx ("By submitting an inquiry, you agree to these terms of usage and limitations of warranty. In particular, you agree not to use this data to allow, enable, or otherwise make possible, dissemination or collection of this data, in part or in its entirety, for any purpose, such as the transmission of unsolicited advertising and solicitations of any kind, including spam. You further agree not to use this data to enable high volume, automated or robotic electronic processes designed to collect or compile this data for any purpose, including mining this data for your own personal or commercial purposes."); http://www.networksolutions.com/whois/ ("By submitting a WHOIS query, you agree to abide by the following terms of use: You agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via direct mail, e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to Network Solutions (or its computer systems). The compilation, repackaging, dissemination or other use of this Data is expressly prohibited without the prior written consent of Network Solutions.").

[8] *See* Avri Doria, Rethinking the Role of ICANN and the gTLD Whois to Enhance the Security and Stability of the DNS, http://forum.icann.org/lists/gnso-dow123/msg01286.html.