COALITION FOR ONLINE ACCOUNTABILITY
WWW.ONLINEACCOUNTABILITY.NET

C/O MITCHELL SILBERBERG & KNUPP LLP ● 1818 N STREET N.W., 8TH FLOOR ● WASHINGTON, D.C. 20036-2406
TEL: (202) 355-7906 ● FAX: (202) 355-7899 ● E-MAIL: INFO@ONLINEACCOUNTABILITY.NET

Comments of

Coalition for Online Accountability on

Whois Policy Review Team Discussion Paper

http://www.icann.org/en/public-comment/whoisrt-discussion-paper-09jun11-en.htm

July 23, 2011

The Coalition for Online Accountability (COA) appreciates this opportunity to respond to the Discussion Paper issued by the Whois Policy Review Team. Our comments can be summarized as follows:

- The gTLD Whois virtual database is a vital public resource, and ICANN's stewardship of it, on the whole, has been ineffective.
- The unchecked proliferation of proxy registration services has contributed significantly to Whois data inaccuracy and has helped to degrade the resource. Reform of the current "system" is urgently needed, perhaps beginning with ICANN enforcement of standards for the operation of proxy services offered in connection with gTLD domain name registration.
- Registries and registrars must assume greater responsibility for accurate Whois data, through the adoption of thick Whois models throughout the gTLD space; data accuracy contractual obligations that flow through from registries to registrars; and making verification of registrant data the norm.
- ICANN's compliance activities need both greater resources and a more proactive re-orientation.

About COA

COA consists of eight leading copyright industry companies, trade associations and member organizations of copyright owners. These are the American Society of Composers,

Authors and Publishers (ASCAP); Broadcast Music, Inc. (BMI); the Entertainment Software Association (ESA); the Motion Picture Association of America (MPAA); the Recording Industry Association of America (RIAA); the Software and Information Industry Association (SIIA); Time Warner Inc.; and the Walt Disney Company. COA has been an active participant in a wide range of ICANN policy development activities, both on its own account and as a member of the Intellectual Property Constituency (IPC). Whois policy has been a particular focus of the ICANN activities of COA and of its predecessor organization, the Copyright Coalition on Domain Names (CCDN).

Introduction: ICANN's Stewardship of Whois

The Affirmation of Commitments spells out the task of the Review Team, which is repeated on page 1 of the Discussion Paper: "to assess the extent to which existing WHOIS policy in the generic top level domains (gTLDs) and its implementation (1) is effective; (2) meets the legitimate needs of law enforcement; and (3) promotes consumer trust." COA suggests that another way to approach this task is for the Review Team to evaluate how effective ICANN has been as the steward of an extremely valuable and socially beneficial Internet resource: the virtual "Whois database" of contact information for second level domain name registrants (and their administrative and technical contacts) in the gTLDs.

The wide range of vital uses of this publicly accessible data is well known; the GAC principles adopted in 2007 catalog seven of them. See http://gac.icann.org/system/files/WHOIS_principles.pdf, paragraph 2.1. It is beyond dispute that **Whois represents a crucial tool for accountability and transparency on the Internet,** enabling right holders, law enforcement, consumer protection groups, and ordinary Internet users to learn something about who is responsible for websites that they or their families visit, and in general to know who they are dealing with online.

When ICANN came on the scene in the late 1990's, the gTLD Whois database for the TLDs generally open to public registration[1] had the following characteristics:

- It was unified. The entire database was held by, and made available by, the monopoly provider of domain name registration services .
- It was accessible 24/7, to all members of the public, without charge, and with virtually no restrictions on use of the data.
- It was fully searchable. Whois users could, for example search by registrant as well as by domain name, and thus identify multiple registrations by the same registrant.
- It had serious problems of inaccuracy. While the first measurements of the degree of inaccuracy did not come until later, there is no doubt that many registrants supplied patently false data, and there was little enforcement of accuracy requirements.

[1] .com, .net, and .org.

Fast-forward through a dozen years of ICANN stewardship of the domain name system, including Whois. How would we characterize the gTLD Whois database today?

- It is fragmented. Not only does each registry manage its Whois data independently; but the two largest gTLDs are operated as "thin registries," with all registrant contact data scattered among 900 + ICANN-accredited registrars.

- It has limited searchability. Few if any domain name registrars offer a fully searchable Whois database to the public as part of their free services. (Of course, some third-party vendors offer this service, to the extent that they are able to aggregate current Whois data from all the registrars and from those registries (all but .com and .net) operating thick Whois services.)

- Whois data remains seriously inaccurate. There have now been some studies quantifying the level of that inaccuracy, most recently the NORC study, commissioned by ICANN, and referenced by the Review Team, which concluded that less than a quarter of Whois records could be considered "fully accurate." See http://www.icann.org/en/compliance/reports/whois-accuracy-study-17jan10-en.pdf, pp. 2-3. The more in-depth we study the accuracy problem, the worse it appears.[2]

- A new and pervasive source of inaccuracy flows from the unmanaged proliferation of so-called proxy and privacy registration services. ICANN's own studies suggest that these account for at least 18% of all gTLD registrations.[3] In the vast majority of these cases, no contact information regarding the actual registrant appears in the publicly accessible Whois data; instead, any contact data appearing there is that of a third party (often, though not always, an alter ego of the registrar) who serves as a proxy. If .proxy were its own gTLD, it would contain 20 million domain names, making it the second largest gTLD in the world, after .com. While proxy services existed at the time ICANN assumed stewardship over Whois, the explosive growth of these services represents a serious threat to the public policy objectives served by accessible, accurate Whois data.

Our conclusion: **on ICANN's watch, the value of the Whois database to the public, and its role in promoting consumer trust, has significantly degraded. Its stewardship of this precious resource, while positive in some respects, has on the whole been ineffective.** Reversing this degradation of Whois is the challenge ICANN must confront.

We understand that, in some cases, these trends were driven by other considerations. For example, the decision to disperse registrant contact data at the registrar level was part of an

[2] For example, the 2005 GAO study, which, as NORC noted, "picked up only the most obvious errors" in Whois data, reported that 7.1% of the Whois data in .com, .net and .org was either patently false, incomplete, or simply inaccessible. The comparable figures for the much broader NORC study were about the same, but NORC went on to report that nearly 30% of the registrations were associated with Whois data that, whether or not patently false, was nevertheless false and either fully or substantially failed an accuracy test. See http://www.icann.org/en/compliance/reports/whois-accuracy-study-17jan10-en.pdf, at 4-5 and Appendix 4.

[3] http://www.icann.org/en/compliance/reports/privacy-proxy-registration-services-study-14sep10-en.pdf.

overall effort to replace the registration monopoly with a competitive marketplace in gTLD registration services. We also recognize that ICANN cannot simply turn back the clock. But we believe this longer-term view is useful, both in evaluating the questions the Review Team has been tasked to address, and in preparing its recommendations for how ICANN's stewardship can be improved in the future.

Viewed from this perspective, we now turn to some of the major challenges facing ICANN. We correlate these to some of the questions posed in the Discussion Paper, though not in the order presented there.

1. Reform Proxy and Privacy Registration Services (see Q. 5)

As noted above, until ICANN is able to bring some semblance of order, predictability and accountability to the current "Wild West" scenario of proxy registrations, it will be impossible to make significant progress toward improving the accuracy of Whois data, so that the service can better fulfill its critical function for Internet users and society as a whole.

COA does not reject the concept of proxy registration in principle, although we encourage the Review Team to study the experience of those ccTLDs (such as .us) that do not permit it (this suggestion responds to Q. 11). We recognize that there may be legitimate reasons, in limited circumstances, why domain name registrants should be permitted to substitute for their own contact details (to be made publicly accessible via Whois) those of a third party. Certainly COA has no concern when the vast majority of registrants, who do not use the registration for abusive purposes, avail themselves of such an opportunity. But common sense tells us that such a mechanism will inevitably and disproportionately prove attractive to registrants who intend to use their domain names to impinge on the rights of others, whether through intellectual property infringements, fraud, or other misconduct.[4] This is fully consistent with the experience of COA members; one association reports that the majority of sites it investigates for engaging in or facilitating high-volume copyright infringement are registered using proxy services. From our perspective, the key is whether a member of the public can expeditiously gain access to the contact information of the actual registrant when it has a bona fide need to do so, including, but not necessarily limited to, the situation in which the domain name is being used to commit copyright or trademark infringement, fraud, or other misconduct.

The current system is clearly inadequate. Section 3.7.7.3 of the Registrar Accreditation Agreement provides that any registrant can "license use of a domain name to a third party," but the licensor "shall accept liability for harm caused by wrongful use of the Registered Name, unless it promptly discloses the current contact information provided by the licensee and the identity of the licensee to a party providing the Registered Name Holder reasonable evidence of actionable harm." This contractual provision has provided the template for nearly all proxy registration services: by signing up for such a service, often in connection with the initial

[4] ICANN staff has already conducted two studies confirming this common-sense intuition, and indicating that proxy registrations are disproportionately used by registrants engaged in abusive behaviors such as spam, and "a range of criminal activities." See http://securityskeptic.typepad.com/the-security-skeptic/2010/04/domainname-privacy-misuse-studies.html.

registration of the domain name, the true registrant designates a proxy service (often, but not always, an alter ego either of the accredited registrar sponsoring the registration, or of a reseller authorized by that accredited registrar) as the "registrant," and enters into a "license agreement" in which the party actually using the registration becomes the "licensee." Whatever contact information is provided by this licensee is held, not in the registrar's Whois database accessible to the public, but in the proxy service provider's files, to which no one has access.

Whether, and under what circumstances, a third party (such as a right holder injured by the use of the domain name) can gain access to this contact information depends on interpretation and enforcement of section 3.7.7.3. Virtually every operative clause of the provision is hotly contested. It is very common for the proxy service provider to refuse to disclose the data, even when presented with evidence of the harm being inflicted, absent a court order, subpoena or similar legal process ordering it to do so.[5] Furthermore, even if there were agreement that what was presented constitutes "reasonable evidence of actionable harm" (which often there is not), there is still controversy about what consequences, if any, would befall a licensor/proxy service that refused to divulge this information. If the licensor were an accredited registrar, would its refusal violate the RAA? What if it were a reseller, without direct contractual privity with ICANN? What if the licensor were simply a registrant: would its failure to disclose its customer when presented with "reasonable evidence of actionable harm" require cancellation of the registration for which it – the licensor – is the official registrant? Would it even justify such a cancellation? Or would the sole remedy available to the third party – which is not a party to the RAA – be to sue the licensor/"registrant"/proxy service for its contribution to the infringement or other tort (or, in some cases, crime) which the "licensee" is allegedly committing through use of the domain name?

In sum, Section 3.7.7.3 of the RAA is a ball of confusion, a weak and ambiguous contractual commitment. More aggressive enforcement of it, while needed, will provide only limited benefits. Even modest efforts to clarify it through a proposed Registrar Advisory from ICANN have collapsed under adamant opposition from registrars. See http://forum.icann.org/lists/raa-subsection-3773-advisory/pdfDyex66DILG.pdf.

In practice, whether a third party who presents "reasonable evidence of actionable harm" to the proxy service provider will learn who is actually "using" the domain name will vary wildly and unpredictably from registrar to registrar, proxy service provider to proxy service provider, "licensee" to "licensee", third party to third party. Such an inconsistent and unpredictable arrangement – it hardly deserves to be called a "system" – is particularly indefensible, since all the third party is seeking is exactly the information that the Whois system is intended and designed to deliver to it quickly, easily, and without expense.

Clearly, **reform of the proxy registration system is long overdue. COA urges the Review Team to recognize this and to call for such reform as a matter of priority.** Models for doing so abound. A redline of the relevant RAA provisions proposed by the Intellectual

[5] Note the comments of the Motion Picture Association of America, noting that only one of the eight proxy registration services providers it has asked to divulge the contact information of operators of piracy sites has consented to do so.

Property Constituency during the last RAA revision negotiations, in 2007, provides one option. http://forum.icann.org/lists/raa-consultation/pdfWpzxprVjNW.pdf. Notably, a drafting team convened by the GNSO Council in 2010, which included participation from registrars, identified this area as a "high priority" topic for further revision of the RAA. See Final Report on Proposals for Improvements to the Registrar Accreditation Agreement, Oct. 18, 2010, at http://gnso.icann.org/issues/raa/raa-improvements-proposal-final-report-18oct10-en.pdf , page 20, items 5-6. Unfortunately, in March 2011, the registrars and registries, voting en bloc, prevented the GNSO Council from taking any action whatsoever on this drafting team's report, and the entire initiative is at an impasse.

One suggestion has been for ICANN to accredit proxy registration service providers, set the ground rules for their operation in the accreditation process, and prohibit registrars from sponsoring registrations by unaccredited providers. A more immediately feasible first step may be to focus on proxy services offered by accredited registrars (or their resellers, for whose actions the 2009 version of the RAA makes the registrars more accountable); by parents, subsidiaries, or affiliates of registrars or resellers; or by anyone, when the proxy service is offered in conjunction with the initial registration process. Among other responsibilities, these registration-connected proxy services would be required to:

- Collect and verify the full set of registrant contact data from the true registrants (whether or not labeled as "licensees" of the proxy service), and keep this data current;

- Disclose at least the same set of data that would otherwise appear in Whois to a third party presenting basic evidence that the registration is being abused to infringe the rights (including intellectual property rights) of others, commit fraud or deceptive practices, or other categories of harm (it should be spelled out that judicial process is NOT a prerequisite for such disclosure);

- Respect firm time limits for responding to such presentations of evidence, and require services that refuse to disclose to specify in what respect they believe the evidence presented is insufficient.

These requirements would be directly enforceable against registrars when they, their subsidiaries or affiliates, or resellers, violate these provisions. Registrars would also face enforcement action if they continue to deal with non-affiliated proxy registration services after being put on notice of material and repeated violations by them of these standards.

COA also believes that a voluntary code of best practices among responsible accredited registrars would be at least as effective a way of reforming the broken proxy registration system as RAA amendments along the lines summarized above, with a significant caveat: so long as not all registrars sign up to the code, the non-compliant registrars will remain a safe haven for bad actors who wish to cloak their misdeeds in anonymity through abuse of the proxy registration option. COA strongly supports the concept of a best practices approach, and is ready to cooperate with registrars and other players in trying to devise one. Realistically, however, the impetus for doing so is not likely to achieve sufficient momentum without the prospect of mandatory compliance with revised RAA provisions on the horizon.

2. Improve Whois Accuracy (Questions 10-11)

The current intolerable levels of inaccurate Whois data flow directly from ICANN's decision to place virtually sole responsibility for Whois data quality on a party with whom it has no contractual relationship: the registrant. Registrars insist that their only contractual obligation is to respond to reports of false Whois data, rather than to verify data accuracy at the time of collection or even to cancel registrations based on false Whois data. The largest registries have even less role to play on Whois data quality currently. This problem will not be solved or even ameliorated until registries and registrars both share responsibility for Whois data quality.

COA recommends the following three steps as crucial in improving Whois accuracy in the gTLDs. All of these already represent existing ICANN policy in some part of the gTLD space, but should be extended more broadly.

(a) Greater involvement of registries through "thick Whois". All but two gTLD registries now employ a "thick Whois" model, in which a publicly accessible Whois database containing registrant contact information is maintained on a centralized basis by the registry operator, as well as on a distributed basis by registrars. In these gTLDs, the registries share responsibility for Whois accuracy (and availability), and the evidence tends to show that thick Whois results are more accessible and more accurate.[6] Unfortunately, the vestigial thin Whois registries are the two largest: .com and .net. While there certainly may be technical issues in transitioning .com and .net to thick registry operation, ICANN should commit to doing so as soon as feasible and should set a timetable for achieving this reform.

(b) "Flow through" obligations to registrars. Registries in three gTLD registries -- .asia, .mobi and .post – are required to hold their registrars to certain Whois data quality standards (as well as to provide fully searchable Whois not only at the registry level, but also for all registrars sponsoring registrations in those domains). Specifically, each of these registries must require registrars to adhere to a compliance review policy, under which registrars must –

- "designate a contact point to which evidence of false or fraudulent contact data may be reported";
- "institute procedures for investigating claims that registrations may contain false information";
- "for registrations found to contain false information, require their speedy and efficient correction, or otherwise cancellation"; and
- allow "interested third parties [to] invoke these procedures." [7]

ICANN should seek to revise all registry agreements to incorporate similar standards.

---

[6] NORC found that Whois data was accessible 100% of the time in registries employing thick Whois, and that the prevalence of patently false or incomplete Whois data was much higher in .com and .net (5.9% in both cases) than in the "thick Whois" registries (.biz, .info and .org) (ranging from 2.4 to 4.4 %).

[7] See http://www.icann.org/en/tlds/agreements/asia/appendix-s-06dec06.htm#6; http://www.icann.org/en/tlds/agreements/mobi/mobi-appendixS-23nov05.htm; http://www.icann.org/en/tlds/agreements/post/post-appendix-S-11dec09-en.htm.

(c) Registrar data verification requirements. Even in the thick registry setting, the registrar is the entity that actually collects registrant contact data. Currently, registrars reject any contractual obligation to ensure that that data is complete and accurate, nor that it remains current; their only obligations, they insist, are to ask the registrant to provide accurate and current information, with no mandatory consequences for failing to do so. There is much that registrars can do to check and verify the data the registrant presents to them – indeed, they surely do so in the vast majority of cases with respect to billing information (credit card data), but not as to data destined for public access via Whois. But ICANN has never explicitly required them to take these steps.

On the other hand, ICANN has made it clear in the new gTLD environment that verification of submitted Whois data (from "authentication of registrant information as complete and accurate at the time of registration" to "regular monitoring of registration data for accuracy and completeness") is the preferred system, whether carried out by registries themselves or via registrars (in which case there must be "policies and procedures to ensure compliance"). ICANN has instructed evaluators to award an extra point to new gTLD applicants that commit to implement such verification (along with other steps to prevent abusive registrations). See http://www.icann.org/en/topics/new-gtlds/evaluation-questions-criteria-clean-30may11-en.pdf, item 28. Not until this approach is made the norm (along with the other steps summarized above) will significant progress toward more accurate Whois data be achieved.

3. Build on Existing Protections for Privacy (Question 4)

The issue of balancing registrant privacy against the need for publicly accessible Whois data has two aspects. The first involves situations in which registrars (or registries) are authoritatively advised that their compliance with ICANN contractual obligations would bring them into conflict with applicable national privacy laws. As the Discussion Paper notes (on page 4), ICANN policy already provides a mechanism for resolving such conflicts. COA is unaware of any need for further policy development in this area.

The second aspect concerns those registrants who require additional privacy protections because of special circumstances, such as those using a domain name to carry out political dissident activities in a repressive society. COA recognizes that this category of registrant exists and should be accommodated, but we believe that the scope of the problem has been greatly exaggerated. There are a growing panoply of ways to establish a robust online presence for the purposes of disseminating dissident views that do not involve registering a domain name at the second level in a generic TLD, and which therefore do not depend upon submission of contact data for public access through Whois. Indeed, with the proliferation of social media, these alternative routes to online presence are multiplying rapidly. On the other side of the equation, it seems likely that a repressive state apparatus would have multiple means to identify and locate anonymous dissidents, and would not need to depend upon publicly accessible Whois for this purpose.

COA supports further discussion to determine the scope of this problem and to identify solutions.[8] We think it is manifestly clear, however, that creation of a vast unmanaged database of tens of millions of effectively anonymous domain names, all but an infinitesimal fraction of which are used for purposes which do not fall within the special circumstances referenced above, is an irrational and socially damaging "solution," one that inflicts far greater costs than warranted upon legitimate e-commerce, consumer interests, law enforcement and the public at large. That is the "system" now in place, due to the interrelated phenomena of widespread proxy registration and unenforced Whois accuracy obligations; and that "system" must be fixed.

4. Step Up Effective Compliance (Questions 6-9, 12-13)

Almost ever since its founding more than a decade ago, COA has called for ICANN to do a better job of enforcing the Whois accessibility and accuracy obligations reflected in its contracts with registrars and registries. We have, simultaneously, called for reform and revision of those contracts to provide clearer and more comprehensive obligations, and to extend them to the wide world of resellers who engage in the domain name registration business but have, in the past, evaded all obligations to ICANN. As explained above with regard to proxy registration services, the current Whois-related provisions of the RAA are, in many respects, ambiguous, weak, or both. We have summarized above some of the changes that should be made in these agreements in order to achieve ICANN's Whois policy goals more effectively.

ICANN's contract compliance capability is certainly improved from what it was a few years ago. However, **it has far to go in order to achieve the necessary "culture of compliance" that will deliver concrete benefits with respect to Whois accessibility and accuracy. COA believes that this will require both resources and re-orientation.**

Especially with the advent of new gTLDs, the contractual compliance burden upon ICANN is about to increase dramatically, at a time when it is not yet effectively enforcing compliance with the contracts that it already has. COA supports the IPC's call to devote one-third of the anticipated ICANN budget surplus from the new gTLD program (i.e., increase in ICANN assets) to contract compliance and enforcement functions.

Perhaps more fundamentally, ICANN should be more proactive in its compliance activities, as well as responding more quickly and forcefully to complaints. We commend the contract compliance staff for deciding to review the Whois Data Problem Reporting System, which has been flawed since its inception and is plagued with problems. We hope that this review will result in a new system that is more receptive to complaints of false Whois data, and can handle higher volumes of them; that more vigorously monitors registrar compliance with their obligations to investigate such complaints; that insists that registrars reject "corrected" contact data that cannot be verified; and that encourages registrars to follow through by expeditiously cancelling registrations associated with uncorrected false Whois data.

5. Clarify Overall Whois Policy (Questions 1-2)

[8] The Whois Misuse study now underway might shed light on this issue. Its results are due in 2012. See http://gnso.icann.org/issues/whois/.

COA appreciates the frustration of some Review Team members that ICANN has never issued a unified document that comprehensively states its policies with regard to Whois. We note, however, that the documents listed on page 4 of the Discussion Paper, read together, outline quite clearly what the ICANN community requires from Whois: that contact data on registrants (and administrative and technical contacts) be publicly accessible through multiple channels, without charge or undue restrictions on use, and that this data be current, complete, and accurate. This is the Whois system that ICANN inherited at its birth; this is the Whois system over which ICANN has had stewardship for more than a dozen years. As noted above, that stewardship has, in many ways, fallen short. COA looks to the Whois Review Team to provide strong recommendations to ICANN to improve that stewardship and to help realize the full potential of Whois for consumers, law enforcement, right holders, and the public at large.

Thank you for considering the views of COA. If there are any questions or further information is needed, please contact the undersigned.

Respectfully submitted,

Steven J. Metalitz, counsel to COA
Mitchell Silberberg & Knupp LLP
1818 N Street, NW, 8th Floor
Washington, DC 20036 USA
Tel: +1 (202) 355-7902
Fax: +1 (202) 355-7899
E-mail: met@msk.com