

RAA NEGOTIATION UPDATE

24 September 2012

This memo describes the current state of the RAA negotiations and the progress of negotiations since Prague. In addition, it highlights key issues remaining open.

ICANN and the Registrars will be jointly conducting a session at the ICANN Toronto Meeting to have further public discussion on the RAA negotiation work.

NEGOTIATION STATUS

Current Situation and Recent Developments

Since the Prague meeting, ICANN and the Registrars have engaged in six additional negotiation sessions, including two all-day, in-person meetings held in Washington D.C. (one of which was attended by Governmental Advisory Committee members and law enforcement representatives). The sessions have been supplemented by information and document exchanges between discussions. The negotiations since Prague have largely focused on the key areas of Whois verification and data retention, which are part of the 12 GAC/law enforcement recommendations. ICANN and the registrars have also continued discussion on the GNSO recommendations and specific requests by ICANN and the registrars, such as supporting DNSSEC and IPv6.

Significant progress has been made, though certain key issues remain open. Those open issues are complex and challenging. ICANN and the registrars are much closer to reaching a negotiated position on Whois verification and data retention than was the case prior to Prague. Because so much of this work has focused on these two areas, we are not producing a new draft RAA at this time for community review. We anticipate that the next full draft of the RAA to be released will be a negotiated document posted for public comment. Though a new draft is not available at this time, a Summary Chart of Status of Negotiations, summarizing key areas of progress, is posted along with this memo. ICANN and the Registrar Negotiating wish to thank the Governmental Advisory Committee and representatives of the law enforcement authorities for supporting the work of the negotiating teams and their participation in the all-day session to provide additional clarifications.

In Prague, we highlighted four critical elements of the law enforcement recommendations:

- (1) verification / validation¹ of Whois data;
 - (2) enhanced collection of information related to registrants (data retention);
 - (3) clarification of registrar responsibility regarding resellers and privacy/proxy services;
- and

¹ For purposes of this memo, “validation” refers to checking the format and completeness of the data, while “verification” refers to checking that the contact points work by sending a message or calling.

(4) creation of contacts for reports of domain name abuse.

In Prague, we reported that there is agreement on the creation of a proxy/privacy accreditation service and operating abuse points of contact. We are now able to report that there is agreement in principle on enhanced data retention obligations. In coordination with law enforcement representatives, ICANN and the registrars have agreed in principle on a dual retention schedule: a six month retention period for some of the more sensitive data, and a two year period after the life of registration retention period for other points of data. Recognizing the importance of addressing privacy and data protection concerns, conversations are focusing now on identifying an appropriate process for evaluating waivers of the data retention obligations in the event of conflicts with national privacy and data protection laws.

The negotiation teams have agreed on enhancements that require the WHOIS entries to be validated for the presence of data and for proper formatting. Both sides have examined the law enforcement agencies' proposals and compared those with the registrars' proposals. With regard to verification, both sides believe the only remaining open issue is whether registrars will be required to verify *either* email or phone number or *both* email and phone number. In addition, and depending on the answer to the either/or question, we have not reached closure on whether the verification is to occur before or after resolution of the domain name. After consultation with GAC members and representatives from law enforcement agencies, ICANN's negotiating position is to support post-resolution verification, *provided that* registrars verify two points of data (telephone AND email). The registrars, on the other hand, have argued that as a first step they should be required to verify only one of the data points (telephone OR email at the discretion of the registrar), with the effect of this change on WHOIS accuracy to be evaluated before further changes are made. While both sides have earnestly endeavored to reach agreement, it is not clear that further negotiations will result in either side changing their position.

Further community discussion on these remaining areas of difference will help determine the appropriate balance of meeting the public's interest and matching the goals behind the law enforcement and GNSO requests.

Other Amendment Topics

Both ICANN and the registrars have proposed additional topics for inclusion in negotiation. The registrars have proposed: (1) a streamlined process, similar to the new gTLD Registry Agreement, for amending the RAA; (2) removal of Port 43 Whois obligations for "thick" gTLDs; (3) aligning the Consensus Policy provisions of the RAA with those contained in the new gTLD Registry Agreement; and (4) automatic accreditation in all new gTLDs.

ICANN has proposed: (1) improved termination and compliance tools; (2) streamlined arbitration; (3) limitation of time for request of stays for negotiations; (4) a prohibition against cybersquatting by registrars and their affiliates; and (5) the inclusion of a revocation clause.

It is ICANN's position that the two sides need to come to resolution of the key topics of Whois verification and data retention prior to publishing a proposed agreement with negotiated amendments in these other areas. Accordingly, the negotiations have focused on Whois verification and data retention and, as described above, have reached substantial but not complete agreement on those elements.

AGENDA FOR PUBLIC MEETING

Key Areas for Community Input

Below we provide some key questions and points of information in advance of community discussions in Toronto – some of which are the same as we posed to the community in Prague. We seek community input on these points. We also seek to continue discussion on how to assure that, when the new RAA is eventually approved, all Registrars will move to the new agreement.

Specific questions and points to help pinpoint the issues are:

Post-resolution Verification

It is our current understanding that law enforcement representatives are willing to accept post-resolution verification of registrant Whois data, with a requirement to suspend the registration if verification is not successful within a specified time period. However, law enforcement recommends that if registrant Whois data is verified after the domain name resolves (as opposed to before), two points of data (a phone number and an email address) should be verified.

Registrars respond that this approach could have a significant negative impact on customer experience without commensurate law enforcement benefits. In particular, registrars have argued that: (1) requiring all registrars to perform phone verification (such as through SMS) could greatly impair registrar ability to serve customers outside of their home country and could impose language challenges in conducting phone verification; (2) verification is likely to result in some customer confusion and will almost certainly increase registrar costs and, if both verification methods are required, the requirement could become cost prohibitive or create barriers to registration services; (3) depending on the country or region, some registrars may prefer to use phone verification methods over email verification methods because of concerns of spam filters, etc; (4) wrongdoers will easily pass either verification test, and neither verification test will have a meaningful impact on deterring or combating illegal activity; and (5) given the uncertainty about the costs and benefits of such verification, registrars advocate an either/or approach and to gather data to enable the community to evaluate the relative merit of each one.

In Toronto, community input is sought on:

- Should the process of registering domain names be changed to perform Whois verification *before* domain names are allowed to resolve? (As the agreement currently stands, validation of would take place prior to resolution.) As part of an

agreement to support a post-resolution verification model, the negotiation teams have agreed in principle to a review of the Whois verification specification after 12 months of registrar adoption, to determine the effectiveness of the new verification obligations, as well as the launch of work to investigate a pilot program for pre-resolution verification. In addition, the registrars have proposed the creation of a cross-stakeholder working group to collect data and inform further enhancements and/or policy development.

- Should registrants be required to have and publish a phone number? (Currently the registrar only has to publish telephone numbers for the administrative and technical contacts, not for the Registered Name Holder.) How else might this impact registrants?
- What are the actual technical and financial burdens for Registrars and the Community in verifying phone numbers and/or email addresses or in conducting such verification before resolution of the domain name?
- What are the costs associated with a requirement to verify both telephone and email contact data, and will such a requirement have a meaningful impact on deterring or combating illegal activity?

Re-verification

The GAC/law enforcement proposal requires some form of re-verification of registrant information. The Whois Reminder Policy has limited effect on Whois accuracy, and some in the community argue that it should be augmented with a re-verification requirement. Conversations have now turned to defining the types of events that should trigger a Registrar obligation to re-verify the certain registrant WHOIS information. Some suggestions of this trigger are: transfers, bounced emails sent by the registrar, a Whois Data Problem Report Service notification, renewal and if registrar has any information suggesting that the contact information is incorrect.

Community input is sought on:

- Should re-verification of Whois information be required on a periodic (e.g., annual) basis as opposed to being event driven? How much of a burden would annual verification impose on legitimate registrants, including those registering large numbers of names?
- Is it appropriate to require registrars to suspend a domain name registration if the annual re-verification is not completed? Are the possible unintended consequences, including liability associated with such suspensions, disproportionate?
- What are other possible events that should trigger a requirement to re-verify registrant Whois data?

- What benefits will re-verification achieve?

Data Retention

Law enforcement representatives appear to be willing to accept a dual-tiered retention schedule, requiring some elements such as transaction data to be retained for a minimum of six months (not six months *after* the expiration of the domain name), while other kinds of data would be kept for two years past the life of the registration. This addresses a key registrar concern that imposing a universal two-year retention requirement would obligate registrars to retain data for longer than it is useable, impose new data retention costs, and create an uneven obligation among registrars, as the data protection/privacy regimes in some jurisdictions would not allow for all data to be maintained for that length of time. The two-tiered schedule is proposed as a schedule that is more likely to be permitted under various data protection regimes, and to assure a consistent application of obligations under the RAA.

The possibility, however, always remains that some registrars may find their data retention obligations to be prohibited by even more restrictive laws. As a result, ICANN and the registrars have discussed various processes under which a registrar might seek a waiver of certain elements of the data retention requirements to the extent that they are in conflict with laws applicable to the registrar. With the assistance of the Governmental Advisory Committee, ICANN and the registrars are evaluating possible modification of the existing “ICANN Procedure For Handling WHOIS Conflicts with Privacy Law” (at <http://archive.icann.org/en/processes/icann-procedure-17jan08.htm>) as a basis for this process. There is concern, however, that as currently drafted, the procedure may only be invoked where a legal proceeding against the registrar has been initiated. The parties believe that in appropriate circumstances it would be preferable to permit a registrar to invoke the waiver process, and for ICANN to consider a waiver request prior to the initiation of a regulatory or judicial proceeding.

- Is the use of a process like the ICANN Procedure for Handling Whois Conflicts with Privacy Law helpful to identify when registrars should be relieved from certain data retention obligations? If no, what process should be used?
- What standards could be imposed to invoke the process, short of requiring the initiation of a formal legal or regulatory process?

Universal Adoption of RAA

The Registrar Negotiating Team has requested, and ICANN agrees, that it is essential to consider how to require and/or incentivize universal adoption of this new RAA. The accreditation model is based upon the principle of uniformity of contracts for all ICANN-accredited Registrars. ICANN and the registrars recognize that those moving to the new RAA will face many new obligations and associated implementation costs. ICANN and the

Registrars are striving to create a globally acceptable improved RAA. Accordingly, the discussion continues on how can global implementation be best achieved.

Some ideas that have been suggested and ICANN seeks community input on these suggestions:

- Provide financial incentive (reduction in both fixed and variable fees) to encourage small and large registrars to migrate to the new agreement. These financial incentives could be structured as tiered incentives, with greater incentives in the near terms to promote early adoption of the form. These financial incentives can also be phased out over time, which would require early adoption of the form to fully benefit from these incentives.
- Assure a fixed period of time within which a new round of negotiations over the RAA will not occur, to provide more business certainty. This would not preclude amendments reached through the processes defined in the RAA.
- Begin limitations on the terms of accreditations and renewals under the 2009 RAA to allow all registrars to move to the new RAA together.
- Create milestones for the phasing in of certain terms under the new RAA, so that more Registrars would be subject to the new RAA when the terms come into effect.
- Use of a Registrar Code of Conduct process to require certain terms to be followed by all Registrars, regardless of whether they are on the 2009 RAA or the new RAA.
- Requiring use of the new agreement when registering names in new gTLDs.

See the companion Summary Chart of Status of Negotiations for more details on key areas of progress in the RAA negotiations.