RDS-WHOIS2 RT Subgroup Report: Safeguarding Registrant Data

DRAFT FOR SUBGROUP USE TO DOCUMENT DRAFT FINDINGS AND RECOMMENDATIONS (IF ANY)

Alan Greenberg (Rapporteur)
Dmitry Belyavsky
Stephanie Perrin
Volker Greimann

5 April 2018

TABLE OF CONTENTS

1 Topic

Subgroup 5 - Safeguarding Registrant Data is tasked with investigating, analyzing, and drafting recommendations (if needed) to address the following Review objective:

Consistent with ICANN's mission and Bylaws, Section 4.6(e)(ii), the review team will assess the extent to which the implementation of today's WHOIS (the current gTLD RDS) safeguards registrant data by (a) identifying the lifecycle of registrant data, (b) determining if/how data is safeguarded in each phase of that lifecycle, (c) identifying high-priority gaps (if any) in safeguarding registrant data, and (d) recommending specific measureable steps (if any) the team believes are important to fill gaps.

To accomplish this objective, the subgroup considered the above objective and concluded:

- Items a), c) and d) are being covered in both the ongoing Next Generation RDS PDP and ICANN Org efforts to comply with data protection laws - specifically, the European GDPR.
- For Item b), currently all WHOIS data is made available publicly. Although this will surely change with regard to WHOIS data associated with natural persons (and likely other groups) as a result of ongoing GDPR compliance efforts, currently there is no protection for that data.
- However, protection against WHOIS (and other) data loss due to Registrar/Registry failure or de-accreditation is required today in the form of Escrow. The subgroup agreed to consider escrow procedures and associated data safeguards used by those who relay and store escrowed data (i.e., Escrow Providers, Registrars and Registries).

2 Summary of Relevant Research

To conducts its research, all members of this subgroup reviewed the following inventoried WHOIS policy and procedure materials, posted on the subgroup's wiki page:

- SAC051, Report on Domain Name WHOIS Terminology (2011)
- SAC054, Report on Domain Name Registration Data Model (June 2012)
- RDS/WHOIS Contractual Requirements - Sections pertaining to Data Safeguards:
- 2013 Registrar Accreditation Agreement (RAA),
  Section 3.6 - Data Retention Specification
- 2014 New gTLD Registry Agreement,
  Specification 2 - Data Escrow Requirements

In addition, the subgroup has requested copies of selected agreements with Escrow providers to better understand what the requirements are on such providers with regard to how data must be protected and how, if applicable, data breaches are reported.

The subgroup is considering reaching out to a sampling of registrars, registries and escrow providers (if any are willing) to learn about how WHOIS data is protected from being changed or erased.

3 Analysis & Findings

For the purposes of this review, "Registrant Data" is defined as all of the data provided by a registrant to fulfil the ICANN WHOIS obligations.

The overall findings were:

a) Currently data is public and there fore there is no effort made to "protect" such registrant data from viewing. That may change as WHOIS policies adapt to GDPR and other legislation, but the details are not known now, and presumably once all of that is complete, we will be incompliance with approriate regulations.

b) Safeguarded not only means to protect from viewing, but to ensure that the data is not lost in the case of a registrar/registry failure, and not unknowingly changed. This includes while the data is held by registrar/registries and by escrow agents.

c) It is known that neither Registry Agreements nor the RAA makes any explicit demands on Registries and Registrars with regard to data protection or actions that must be taken in the case of a discovered data breach (in appropropriate access/change but unauthorized third parties). ICANN's agreement with escrow providers do required that they " use commercially reasonable efforts and industry standard safeguards to protect the integrity and confidentiality of Deposits". But they do not explicitly require that both the registrar/registry and ICANN be notified of a breach in a timely manner.

4 Problem/Issue

Safeguarding data includes ensureing that it cannot be accessed or changed except as duly authorized.

Traditionally, all RDS data is public. Under GDPR and similar legislation, some or all of that data may no longer be collected or publicly available. Exactly what data may be subject to these new rules is under discussion elsewhere and will not be addressed by the RDS-WHOIS2-RT. Registries and registrars are not explicitly required to use commercially reasonable and industry standard safeguards nor are any parties required to notify ICANN in the event that a breach is discovered.

5 Recommendations

Recommendation 1: ICANN should contract with an [external] data security expert(s) to identify reasonable and justifiable requirements to place on registrars and in relation to how data is protected from unauthorized access or alteration while under their control. ICANN should similarly consider whether [or require?] any such breaches that are discovered must be reported to ICANN, and in the case of escrow providers, reported to the egistrar/registry that provided the data.

In carrying out this review, the external consultants should consider the comparable requirements within the GDPR, as many ICANN contracted parties must already adhere to those.

If changes are deemed to be required based on the results of the above-reqoimmended studies, ICANN must either negotiate appropriate contractual changes or initiate a GNSO PDP to consider effecting such changes.

Findings: To be completed once we have access to contracts between ICANN and escrow providers and Excrow providers and contracted parties.

Rationale:
If ICANN has a requirement to safeguard registrant data, as Articles 4.6(e)(ii) and 4.6(e)(iii) imply, then ICANN has an obligation to ensure that its contracted parties act accordingly.

Impact of Recommendation: This recommendation will impact data security and potentially registrants whose data is collected in conjunction with gTLD domain registrations. By helping to ensure that such data is not altered inapprpriately, their domain names and assocated assets are protected. The recommendation could impose additional contractual requirements on registrars and registries.

Feasibility of Recommendation: The RT believes that this recommendation is both feasaible and necessary.

Implementation:
To Be Completed

Priority: [If only 5 recommendations could be implemented due to community bandwidth and other resource constraints, would this recommendation be one of the top 5? Why or why not?] TBD

Level of Consensus
TBD