Registration Directory Service (RDS-WHOIS2) Review

Draft Report including F2F#3 agreements and action items

OBJECTIVE 5 SUBGROUP REPORT - SECTION 7 ONLY
FOR ALAN TO PROVIDE REDLINED UPDATES

RDS-WHOIS2 Review Team
30 July 2018

ICANN

7 Objective 5: Safeguarding Registrant Data

[SUBSECTION NUMBERS WILL BE ADJUSTED WHEN ADDED BACK TO MASTER DOC]

1.1 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).

1.2 Summary of Relevant Research

To conduct 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.

1.3 Analysis and 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 therefore 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 in compliance with appropriate regulations. The end result is that registrant data, at least in some jurisdiction, will be significantly better protected from access than it is today.

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) ICANN's agreements with Registrars, Registries and Escrow providers commit them to varying levels of protecting data in their custody and reporting breaches.

- The 2013 RAA section 3.7.7.8 requires registrars to take "reasonable precautions" in protecting data and section 3.2 requires them to report data breaches to ICANN.
- The standard Registry agreement section 2.18 requires registries to take "reasonable steps" to protect data but does not require that ICANN be notified of data breaches.
- The agreement with Escrow providers section 4.1.12 requires that providers use commercially reasonable efforts and industry standard safeguards. It does bot require that ICANN be informed of data breaches.

Many local laws and regulations require specific standards in data protection and breach notification but details may vary, and in the case of breach, it is not clear whether it is ICANN or the registrant that may need to be notified.

1.4 Problem/Issue

Safeguarding data includes ensuring 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.

1.5 Recommendations

Recommendation SG.1:
The ICANN Board should require that the ICANN Organization, in consultation with data security expert(s), ensure that all contracts with contracted parties (to include Privacy/Proxy services when such contracts exist) include uniform and strong requirements for the protection of registrant data and for ICANN to be notified in the event of any data breach. The data security expert(s) should also consider and advise on what level or magnitude of breach warrants such notification.

In carrying out this review, the data security expert(s) should consider to what extent GDPR regulations, which many but not all ICANN contracted parties are subject to, could or should be used as a basis for ICANN requirements.

The ICANN Board must either negotiate appropriate contractual changes or initiate a GNSO PDP to consider effecting such changes.

Findings: ICANN's agreements with contracted parties have inconsisten requiremenbts regarding the protection of registrant data, and in several cases, no requirement that it be notified in the case of data breach..

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 all 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 inappropriately, their domain names and associated assets are protected. The recommendation could impose additional contractual requirements on registrars and registries.

If this recommendation is not addressed, ICANN Contractual Compliance has no ability to either audit that reasonable efforts are being used to protect data, nor to be aware of serious problems with how its contracted parties are protecting such data.

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

Implementation: Implementation should ensure uniform and appropriate protection of registrant data by all contracted parties along with due notification of ICANN in the event of breaches and the ability of ICANN Contractual Compliance to audit such actions and take action in the case of non-compliance. The review team knows of no current effort to enact such change, but it should be completed within one year of the this recommendation being accepted.

Priority: Medium-High

Level of Consensus: Full

1.6 Possible impact of GDPR and other applicable laws

GDPR require industry standard protect and notification of breach, although it is not clear whether ICANN would be one of the notified parties in all cases. It is unlikely that implementation of this recommendation would cause and non-compliance with GDPR.

ICANN.ORG