Business Constituency (BC) Response to Draft Addendum to the EPDP Phase 2 Report
5-May-2020

Overarching concerns (entered as response to final question)

The new policy is inadequate on the most basic level, making it unfit for purpose to "ensure compliance with the GDPR while maintaining the existing WHOIS system to the greatest extent possible."[1] Accordingly, the BC will have a difficult time supporting the EPDP's proposed outcomes, for the following reasons:

- GDPR has been consistently and inappropriately over-applied to impact jurisdictions and data subjects outside the EU due to ICANN allowing "flexibility to Registry Operators and Registrars to choose to apply the requirements [of the GDPR] on a global basis where commercially reasonable to do so or where it is not technically feasible to limit application of the requirements to data governed by the GDPR."[2] While this flexibility may have been necessary at the outset of ICANN's new Whois policy implementation to quickly pivot to address the GDPR, the EPDP team -- chartered to review and tweak that policy -- has proposed no remedies or adjustments that would "right-size" this unnecessary and overly broad application of the GDPR. Not only does this deny those with legitimate reasons access to data (data that is at the heart of maintaining internet security and stability and not meant to be covered by the GDPR), such over-application has blunted the potential outcomes of the EPDP and granted cover to bad actors online.
- The EPDP team has failed to meet its charter obligations. The team has consistently sought to block data access in nearly all scenarios, while failing to answer operational questions it was chartered to address. For example:
    - The Whois system has not been preserved "to the greatest extent possible" And, instead, the EPDP seemed to constantly seek the opposite outcome even where the GDPR and other laws supported otherwise.
    - Fundamental questions of data controllership and purpose for collection of data have not been answered, making policy output flawed, if not entirely useless under a GDPR analysis.
    - Fundamental GDPR tenets, such as application to natural persons only and not legal persons were ignored or deemed "out of scope", making policy output flawed under a GDPR analysis.
    - Common Whois use cases have not been properly identified or included in discussions to form the basis of policy output.
    - There's been no commitment to prompt responses to volume data requests for cybersecurity needs or as otherwise necessary to perform basic counter-DNS abuse functions.

[1] https://www.icann.org/news/blog/data-protection-privacy-issues-update-more-details-published-on-icann-proposed-interim-model

[2] See ICANN's Temporary Specification for gTLD Registration Data: https://www.icann.org/resources/pages/gtld-registration-data-specs-en

    - Many important issues pushed to Phase 2 of EPDP work were simply ignored or later argued to be "out of scope" and left unaddressed.
- The Standardized System for Access and Disclosure (SSAD), as proposed by the EPDP, is not a useful system because the decision making is decentralized. Rather, in operational reality, it's more of a ticketing system that eases the intake burden on data controllers (currently assumed to be Registry Operators and Registrars) but provides no real benefit to users. This is in contravention of guidance from the Data Protection Authority[3] and the European Commission[4] about their preferences for such a model that would, at a minimum, centralize the Whois system.
- There is no remedy envisaged to address instances where legitimate data requests are being denied. There needs to be set guidance on how legitimate and lawful requests are fulfilled. Many such requests are being unnecessarily denied today, and nothing about the proposed EPDP policy or SSAD would change that outcome. ICANN Org must be able to take compliance action to remedy situations where legitimate data requests are routinely being denied or outright ignored.
- Expanded use cases for automation have been dismissed by the EPDP team and those omissions will hobble the SSAD. It is critical these use cases be immediately added as part of the SSAD if it is to meet global needs. Use cases include:
    - Law enforcement agency in same jurisdiction as contracted party
    - Request for city field (only)
    - Registration record contains no personal data and already has been disclosed
    - Registration record already has been disclosed under the same authorization assertions to a requestor of the same type
    - Cases of a "clear cut" trademark claim
    - When identifying the infrastructure involved in botnets, malware, phishing, and consumer fraud
    - Data subjects have consented to make their registration data public
    - Request for data from a UDRP/URS provider
    - Request for data from ICANN Contractual Compliance, in support of compliance-related investigations
- The EPDP has overlooked Section 4.2 of Appendix A of the Temporary Specification, which states that:

  4.2. Notwithstanding Section 4.1 of this Appendix, Registrar and Registry Operator MUST provide reasonable access to Personal Data in Registration Data to a third party where the Article 29 Working Party/European Data Protection Board, court order of a relevant court of competent jurisdiction concerning the GDPR, applicable legislation or regulation has provided guidance that the provision of specified non-public elements of Registration Data to a specified class of third party for a specified purpose is lawful. Registrar and Registry Operator MUST provide such reasonable access within 90 days of the date ICANN publishes any such guidance, unless legal requirements otherwise demand an earlier implementation.

[3] See https://www.icann.org/resources/pages/h/en/system/files/correspondence/odonohue-to-marby-03may19-en.pdf

[4] See European Commissioner Thierry Breton's answer given on behalf of the Commission to a question from a Member of the European Parliament : https://www.europarl.europa.eu/doceo/document/E-9-2020-000826-ASW_EN.html#def1

This provision is necessary to incorporate into any EPDP policy to ensure that a new policy adjusts automatically in situations where legal clarity under GDPR or other applicable law is received after the EPDP concludes its policy work.

The BC must take the opportunity here to also highlight important policy proposals made by Interisle in its study that have not yet been included in the EPDP team's output that would not only improve the team's work product, but would constructively benefit the user community without violating the tenets of GDPR. Namely:

- Steps for effective RDAP implementation:
  - ICANN Org should expeditiously publish a plan, subject to public comment, for fully retiring Whois in favor of RDAP, including reasonable timelines with milestones and deadlines to meet.
  - Registrars must be required, via new RAA language, to serve registration data (equivalently, regardless of the access mechanism, and according to meaningful SLAs) for all sponsored domains, across all gTLDs.
  - ICANN Org should create a support program for RDAP end users, including a comprehensive toolkit.
  - Contracted parties must provide a free, web-based output mechanism on their respective websites, configured for easy human understanding and use. This requirement, and its associated SLAs, should be codified in contracts (see below regarding contract enhancement).
  - Registrars must come to parity with registries in terms of obligations to publish monthly RDAP query activity.
  - ICANN's compliance monitoring function should verify that RDAP services are responding with correctly formatted and complete data, including all required fields.
  - IANA should publish changes to registry and registrar base URLs into the RDAP Bootstrap Registries within 24-48 hours of update; PTI must set and publish SLAs and performance metrics for these functions.
- Compliance: ICANN must enhance and enforce its contracts in ways it historically has not:
  - Solicit community input regarding constructive modifications to the RAA (last updated in 2013) and RA (last updated in 2012), particularly concerning the area of DNS abuse, and enter into negotiations with contracted parties to effect appropriate changes.
  - Revise agreements so that rate-limiting access to public data is not permitted.

Finally, the BC supports the GAC's comment on this addendum. The BC finds the GAC's positions (treatment of legal person data, registration data accuracy, treatment of privacy/proxy registrations, and anonymized email) persuasive and oriented toward successful outcomes for the EPDP that will benefit the internet community, and urges the EPDP team to favorably consider them.

Preliminary Recommendation #20. Display of information of affiliated vs. accredited privacy / proxy providers

In the case of a domain name registration where an accredited privacy/proxy service is used, e.g., where data associated with a natural person is masked, Registrar (and Registry, where applicable) MUST include the full RDDS data of the accredited privacy/proxy service in response to an RDDS query. The full privacy/proxy RDDS data may include a pseudonymized email.

- This falls well short of the public's interest in data disclosure for reasonable purposes. ICANN has no choice -- it must restart the implementation team for Privacy/Proxy Services Accreditation Issues (PPSAI). After three years, the settled PPSAI policy needs to move into implementation immediately.
- Cybercriminals are benefiting from the stalled privacy/proxy policy. Meanwhile, the rest of the community -- even ICANN itself -- is suffering from the stall.
- ICANN Org is turning a blind eye to the growing use of privacy/proxy services to facilitate fraud and abuse.
- The EPDP is not addressing privacy/proxy registrations. Without implementation, there will be a gaping and widening hole in any Whois policy coming from the EPDP on what amounts to approximately 31% of domain registrations -- or approximately 110 million (based on trends from UDRP filings for the last three years).

The BC recommends the following wording for a policy recommendation: *ICANN Org MUST direct the Privacy/Proxy Services Accreditation Issues IRT to promptly conclude its implementation work. That IRT output must then be incorporated into the EPDP policy once completed to dictate how an accredited privacy/proxy service is used under the policy.*

Preliminary Conclusion – Legal vs. Natural Persons

There is a persistent divergence of opinion on if/how to address this topic within the EPDP Team. As a result, the EPDP Team will consult with the GNSO Council on potential next steps.

- Lack of differentiation between legal and natural persons is an over-application of GDPR and breaks with one of the core tenets of the GDPR.
- The legal vs. natural question has persisted throughout the life of the EPDP; it's well known to the community that such a distinction can be made and is an intended underpinning of the GDPR.
- The legal vs. natural persons distinction is a Phase 1 issue that was promised to be addressed in Phase 2. However, various parties participating in the EPDP have thus far successfully blocked policy development on this matter. Now is the time to handle what should be a non-controversial issue to fall in line with the GDPR -- which is the point of this exercise.
- We object to the legal vs. natural person distinction being punted to GNSO Council, where we fear it would be intentionally de-prioritized or buried.

The BC recommends following legal advice from Bird & Bird which, upon implementation, would allow contracted parties to rely on self-identification by the registrant to determine legal vs. natural status and the ability to reveal. To further streamline the process, the BC recommends automated responses to data queries for legal persons.

The BC suggests the following wording for a policy recommendation: *In the case of a domain name registration where the registration data has been self-identified as that of a legal person, a party's legitimate request for disclosure MUST be granted, preferably on an automated basis.*

Preliminary Conclusion – City Field Redaction

No changes are recommended to the EPDP Phase 1 recommendation that redaction must be applied to the city field.

- The BC would like to see automated use case where just the city field would be returned in appropriate situations, such as where the jurisdiction for legal claims is to be established.

Preliminary Recommendation #21. Data Retention

The EPDP Team confirms its recommendation from phase 1 that registrars be required to retain only those data elements deemed necessary for the purposes of the TDRP, for a period of fifteen months following the life of the registration plus three months to implement the deletion, i.e., 18 months. This retention is grounded on the stated policy stipulation within the TDRP that claims under the policy may only be raised for a period of 12 months after the alleged breach (FN: see TDRP section 2.2) of the Transfer Policy (FN: see Section 1.15 of TDRP). For clarity, this does not prevent requestors, including ICANN Compliance, from requesting disclosure of these retained data elements for purposes other than TDRP, but disclosure of those will be subject to relevant data protection laws, e.g., does a lawful basis for disclosure exist. For the avoidance of doubt, this retention period does not restrict the ability of registries and registrars to retain data elements for longer periods.

- The BC notes there will be cases in which investigations require access to data beyond the proposed 18 month timeframe put forth in the recommendation. We therefore recommend a retention period of at least two years.

Preliminary Conclusion – OCTO Purpose

Having considered this input, most members of the EPDP Team agreed that at this stage, there is no need to propose an additional purpose(s) to facilitate ICANN's Office of the Chief Technology Officer (OCTO) in carrying out its mission. Most also agreed that the EPDP Team's decision to refrain from proposing an additional purpose(s) would not prevent ICANN org and/or the community from identifying additional purposes to support unidentified future activities that may require access to non-public registration data.

- This is acceptable under the assumption that Purpose 2 will cover any necessary processing by ICANN of personal data; this includes OCTO, Compliance, assistance with cyber investigations, etc. If the assumption is not correct, this outcome is unacceptable.
- Further, the BC urges the EPDP team to recognize that ICANN Org has identified its own unique role with regard to the registration database. Quoting from ICANN Org's comment to the European Commission on the application of GDPR: "ICANN's role in providing the technical coordination of the globally distributed WHOIS system is a unique matter, considering the public interest nature of WHOIS, and responsibilities relating to the WHOIS system are encapsulated in

ICANN's Bylaws." ICANN Org goes on to say: "Developing and implementing a global system to balance the law's data protection requirements with the legitimate interests of parties seeking access to nonpublic gTLD registration data, including the important public interest goals that legitimate access to non-public registration data serves for **all parties involved**, presents a number of challenges." (Emphasis added.) Implicit here is the periodic need for ICANN Org itself, including OCTO, to access WHOIS records in support of this unique mission. The community should recognize this admission by ICANN Org and take care not to abridge this capability.

Preliminary Conclusion - Feasibility of unique contacts to have a uniform anonymized email address

The EPDP Team received legal guidance noting that the publication of uniform masked email addresses results in the publication of personal data; therefore, wide publication of uniform masked email addresses is not currently feasible under the GDPR.

- The BC supports neither this recommendation nor the interpretation of legal guidance purporting to support it. Anonymization of email addresses is designed precisely to avoid disclosure of personally identifiable information while still offering a reasonable method for contacting the registrant as necessary.
- Registrant contactability should be enhanced:
    - ICANN should ensure registry and registrar RDAP output includes a method for contacting the current registrant.
    - Registrars should take measures to ensure messages forwarded to domain contacts are not blocked as spam but affirmatively received by intended contacts.
    - ICANN should require automation of contact mechanisms, without resorting to the use of generic addresses.
    - ICANN should regularly test contact forms and anonymized emails to determine if operational.

Preliminary Conclusion – Accuracy and Whois Accuracy Reporting System

Per the instructions from the GNSO Council, the EPDP Team will not consider this topic further; instead, the GNSO Council is expected to form a scoping team to further explore the issues in relation to accuracy and ARS to help inform a decision on appropriate next steps to address potential issues identified.

- The European Commission has (correctly) said accurate data isn't an optional obligation of GDPR -- it's essential. A reminder that Article 5(1)d of the GDPR stipulates that personal data shall be "*accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*." This is critical to a workable registrant data system and an obligation for controllers who collect, store, and process personal data.
- Data accuracy is an issue the EPDP team promised action on during Phase 1 as a deliverable in Phase 2. That promise has been broken.

The BC suggests the following wording for a policy recommendation:

ICANN Org MUST address registration data accuracy by:

- resuming its registration data accuracy studies;
- Obtaining contact data for Compliance department use in performing data accuracy compliance checks;
- Implementing enforceable cross-field validation check requirements for Registrars and Registries, per the terms of the 2013 RAA; and
- Requiring enhanced verification requirements for registrants – particularly registrants identified as engaged in DNS abuse, online crimes and IP infringement (following the methodology used in conducting the accuracy tests).

Preliminary Recommendation #22. Purpose 2

The EPDP Team recommends the following purpose be added to the Phase 1 purposes, which form the basis of the new ICANN policy:

> *Contribute to the maintenance of the security, stability, and resiliency of the Domain Name System in accordance with ICANN's mission.*

The BC has no comment on this recommendation.

This comment was drafted by Mason Cole and Alex Deacon, with edits from Claudia Martinuzzi.

It was approved in accord with our charter.