Minority Statement of the ICANN Business Constituency on the EPDP Phase 2A Final Report[1]

10-Sep-2021

Introduction

This minority statement is submitted on behalf of the ICANN Business Constituency (BC).[2]

The BC is an ardent supporter of privacy rights and the protective intent of the GDPR. However, in the context of the EPDP team's work on this expedited policy development process (EPDP) -- a team that was explicitly directed to "preserve the WHOIS database to the greatest extent possible" while complying with privacy law -- the resulting policy exceeds what is necessary to protect the data of natural persons.

The EPDP Team Phase 2A was tasked by the GNSO Council to focus on two specific topics: 1) the differentiation of legal vs. natural persons' registration data and 2) the feasibility of unique contacts to have a uniform anonymized email address. Our comment focuses on the legal vs. natural distinction, the lack of enforceable outcomes and, importantly, and on the critical need to respond to European legislative progress that will impact developed policy, or the lack thereof.

As previously stated, the BC strongly believes that *optional* differentiation of legal vs. natural persons is inadequate and that ICANN policy must require such differentiation to ensure the security and stability of the global DNS.

In sum, the Phase 2A recommendations, by *not* making the distinction between legal vs. natural persons, results in a significant number of records being redacted or otherwise unavailable. This is distressing, and even frustrating, given the well-known prevalence of online harms. Such frustration was well-documented in the recent survey by the Messaging, Mobile and Malware Anti-Abuse Working Group (M3AAWG)[3], which detailed the substantial limitations of current access to non-public domain name registration records and affirmed that the solutions currently discussed by ICANN would *not* meet the needs of law enforcement and cybersecurity actors.

While the EPDP team has designated its recommendations as supported by "consensus", the BC restates that it does not support Phase 2A outcomes, does not support a "consensus" designation, and here provides justification for its dissent.

---

[1] 3-Sep-2021, EPDP Phase 2A Final Report, at https://mm.icann.org/pipermail/gnso-epdp-team/attachments/20210903/4c231c0a/EPDPPhase2A-FINALREPORT-3September2021003-0001.pdf

[2] *Prior BC comments and minority report on EPDP Phase 2 include:*

- *BC and IPC submitted a joint minority statement for EPDP Phase 2.*
- *BC Phase 2A Initial Report comments*

[3] https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf

BC's View on EPDP Phase 2A Final Report

A core tenet of ICANN's mission is to establish consensus policy that contributes to the security and stability of the DNS and to rigorously enforce any obligations resulting from such policy. However, the BC observes a recent trend -- particularly pronounced in Phase 2A Working Group (WG) deliberations and outcomes -- toward reliance on "optional" obligations (e.g., the use of "should" and "may" in recommendation language) that skirts obligations and does not firmly commit to maintain security and stability. Further, there is growing reliance on the issuance of guidance instead of binding policy, leaving significant latitude for contracted party compliance and weak, watered down, and probably unenforceable policy. This is an unfortunate outcome. The BC believes that the ICANN community should spend time on policy that will uniformly apply to *all* registrars and registries -- not merely to an undefined subset, acting on their own whims.

In fact, the BC notes that other than the first part of Recommendation #1 (which obligates ICANN to coordinate with the technical community to develop technical standards to facilitate differentiation between legal and natural person registration data), the EPDP Phase 2A Final Report contains no real policy and places no enforceable obligations on contracted parties. This represents an unfortunate failure of the multistakeholder process.

The EPDP team's "consensus" designation for the final report does not reflect the deep divisions in working group outcomes. It is clear that a significant segment of WG membership, as well as a sizable part of the ICANN community, find Phase 2A outcomes to be inadequate. This division should not be overlooked, even as the WG insists on positioning this report as one supported by consensus.

Requiring a Distinction between legal and natural persons

We reiterate that the inability of Internet users to identify with whom they are doing business online, and the increasing inability of law enforcement, cybersecurity, and legal professionals to identify criminal actors online through their domain name registration data, continues to severely undermine ICANN's security and stability mandate. Thus, the interests of these users are not adequately reflected in the policy.

The EPDP Phase 2A team's inability to reach consensus on recommending changes to Phase 1 Recommendation #17.1, and its failure to "determine and resolve the Legal vs. Natural issue" in its deliberations as required by the Phase 1 policy, does not mean the policy defined in Phase 1 Recommendation #17.1 should stand or should become the "default" ICANN policy. In fact, the opposite has occurred. Because the Phase 2A team was unable to reach consensus on this recommendation, we believe the record should state that consensus opinion did not and still does not exist that would permit optional legal vs. natural differentiation by registrars and registries.

NIS2 Directive

The maturation of theNIS2 Directive signals that the European Parliament not only will address and impact the issue of legal vs natural differentiation, but other WHOIS-related policy, including accuracy, critical data elements, timely publication of non-personal data, and timely reply to legitimate access seekers. ICANN should be keenly aware that key stakeholders, including regulatory authorities in Europe and the United States, are closely monitoring the European Parliament's engagement on these issues via NIS2. Forthcoming opinions and decisions by tribunal and privacy regulatory authorities are likely, and could accelerate as a result of the NIS2-related proceedings. It is distinctly possible that the progression of NIS2 could rapidly overtake ICANN policy development, and ICANN will need to revisit the impact of NIS2 once it is adopted.

ICANN should thus be obligated to properly respond to the NIS2 Directive when it is adopted by the European Union. That gives time for ICANN to update its contracts and policies before NIS2 is first transposed into EU member states' laws. Failure to do so will likely result in a fragmented and inconsistent industry approach to the obligations of the Directive.

Recommendation #1

The BC does not support this recommendation.

While we support an obligation for ICANN to define a standard technical mechanism to facilitate differentiation between legal and natural persons' registration data, the BC regrets the lack of obligations of contracted parties to make use of this field, or even to indicate whether they have differentiated. The failure to require use of this technical mechanism will not result in a consistent and reliable RDDS, and is a missed opportunity to reduce the number of requests for non-personal data which has been unnecessarily redacted, such as the contact data for unaffiliated privacy/proxy services. This outcome falls well short of the needs of those involved in the investigation of DNS abuse, cybercrime activity, intellectual property violations, and other activity that threatens consumer welfare.

As stated above, the BC believes strongly that ICANN must take action to update the EPDP policy when the NIS2 Directive has been adopted by the European Union.

Recommendation #2

The BC opposes Recommendation 2 on procedural grounds and with regard to its specific recommendation.

Procedurally, in violation of ICANN Bylaws and the EPDP Phase 2 Charter, the EPDP Phase 2A team inexplicably devoted significant time to developing guidance rather than binding consensus policies. A subset of WG membership effectively "ran out the clock," dedicating most

of its efforts to creating guidance, thereby delaying until the final weeks of Phase 2A any meaningful and robust discussion of how to create binding consensus policies.

The ICANN Bylaws Annex 2-A specifies the process for producing guidance, which requires the formal initiation of a Guidance Process by the GNSO Council. This process was not followed and, as a result, cannot justifiably produce guidance.

Because of this, the policy defined in Recommendation #2 should be adopted as consensus policy and not merely "guidance", and appropriately enforced.

With regard to the specifics of the recommendation, the BC finds that it also is weak and unenforceable, further hobbling the usability of domain name registration data for legitimate purposes. The recommendation should require contracted parties to follow the tenets of Recommendation 2.

Finally, we note that there is an error on page 20 of the Final Report, which should be corrected as follows:

> *"This generally allows for **publication** ~~disclosure~~ of legal persons' data because it is outside the remit of GDPR; however, when processing legal persons' data, Contracted Parties should put safeguards in place to ensure that personally identifying data about a natural person is not **published** ~~disclosed~~ within data marked as a legal person, as this is an example of information that is within the scope of GDPR."*

These clarifications are needed to ensure consistency with the recommendations from the EPDP Phase 1 report -- namely, that information of a natural person ***can be disclosed upon request***, for legitimate purposes, provided that an appropriate legal basis exists under GDPR.

Recommendation #3

The BC observes that this recommendation does not define any enforceable obligations on the part of any specific party, nor does it encourage development of such. Recommending that work on a Code of Conduct be "considered" by "any possible future work within ICANN" is vague and unenforceable, and it leaves unattended community priorities that deserve due attention.

Accordingly, the recommendation should encourage ICANN to commence a process for establishing a Code of Conduct. Should ICANN do so, the BC would object strongly to any process that would not involve all ICANN stakeholders. The definition and development of a Code of Conduct must be carried out in an open, transparent and inclusive manner and must not be developed outside of the ICANN multi-stakeholder process (e.g. via closed-door negotiations between ICANN Org and contracted parties).

Recommendation #4

It was unfortunate that the EPDP team didn't devote adequate time to address this important topic. The BC continues to believe that a registrant-based pseudonymous email address should be ***required*** to facilitate the investigation of DNS abuse by enabling contactability and cross-referencing of registrations by registrants.

Once again the BC regrets that this recommendation does not define any enforceable obligations on contracted parties, leaving significant gaps between the recommendation and practical implementation. Recommending that contracted parties evaluate legal advice and assess risks, benefits and safeguards is likely to result in an over-cautious, weak, and ultimately ineffectual policy.

This comment was authored by Alex Deacon, Margie Milam, Steve DelBianco, Mark Svancarek, Drew Bennett, and Mason Cole. It was approved in accord with our charter.