Minority Statement of the Business Constituency (BC) and Intellectual Property Constituency (IPC) on the EPDP Phase 2 Final Report

The EPDP Phase 2 Final Report fails to deliver a System for Standardized Access that meets the needs of its users. Accordingly, the Business Constituency (BC) and the Intellectual Property Constituency (IPC) must dissent.

As noted in our statement on the EPDP Phase 1 Final Report, the BC and IPC are staunch supporters of the ICANN bottom-up, consensus-driven multistakeholder model, as shown by our good faith, active participation in this EPDP. Phase 2 of the EPDP was chartered to create a standardized system, with twin goals of protecting registrants' personal data and providing users with consistent, timely and predictable access to registrant data when users have a need to process this data lawfully for their legitimate purposes. Because the Phase 2 Final Report fails to do so, the Phase 2 Final Report is unacceptable.

Shared Concerns

The IPC and BC support privacy protection for personal data, and privacy law seeks to strike a balance between the individual right to privacy and other legitimate interests. Unfortunately, the Phase 2 Final Report fails to strike this balance. This failure is a detriment to those protecting their own fundamental rights and to those acting in the public interest or other legitimate interests. The interests of BC members include promoting user confidence in online communications and business interactions (as advanced by the EU NIS Directive, for example). The interests of IPC members include protecting consumers from phishing, dangerous counterfeit products, and other fraud as provided in Article 38 of the EU Charter of Fundamental rights, as well as protecting intellectual property as provided in Article 17 Section 2 of the EU Charter of Fundamental Rights.

The IPC and BC note that the Phase 2 Final Report fails to address several concerns raised by the European Commission and Belgian Data Protection Authority (DPA), as well as ICANN's own advisory committees: the Government Advisory Committee (GAC) representing law enforcement and consumer protection interests, the At Large Advisory Committee (ALAC) representing internet end user interests, and the Security and Stability Advisory Committee

(SSAC) responsible for advising the ICANN Board on matters relating to the security and integrity of the internet's naming and address allocation systems.

Concerns shared with the European Commission and Belgian DPA

The European Commission[1] urged *"ICANN and the community to develop a unified access model that applies to all registries and registrars and provides a stable, predictable, and workable method for accessing non-public gTLD registration data for users with a legitimate interest or other legal basis as provided for in the General Data Protection Regulation (GDPR)."* The European Commission stated that it considered this "*vital and urgent*" and urged ICANN to "*develop and implement a pragmatic and workable access model in the shortest timeframe possible…*" The Belgian DPA, which is ICANN's supervisory authority due to its EU establishment in Belgium, called the centralized model a "*better, 'common sense' option in terms of security and for data subjects.*"[2] Unfortunately, the Phase 2 Final Report fails to provide a method for access at all, let alone a method that could be described as "*stable, predictable, and workable.*" On the contrary, the Phase 2 Final Report merely provides for a central location to submit requests. In so doing, it rejects the Belgian DPA's guidance in favor of leaving the decision about whether or not to disclose data at the discretion of over two thousand separate contracted parties, none of whom are required under ICANN's contracts or policies to employ legal counsel, a data protection officer, or a privacy professional.

BC and IPC Concerns that are shared by the GAC

We also share the concerns of the GAC on the EPDP team's failure to address issues of data accuracy and the distinction between legal and natural persons. In their June 22 letter to the GNSO Council[3] the GAC noted that "*These issues are critical to the public interest. Not addressing these issues as part of the current EPDP risks an incomplete system that will lack key capabilities that promote public safety. Moreover, the failure to deal with these important issues throws doubt upon the legitimacy and effectiveness of the GNSO policy development process to address issues of importance to non-GNSO stakeholders and the public interest.*" Unfortunately, the GAC's pleas were ignored in Phase 2. Although the GDPR requires data accuracy, the GNSO Council removed accuracy from the remit of the EPDP Phase 2 work, and the Phase 2 Final Report failed to address the need to distinguish between legal person and natural person registrants.

BC and IPC Concerns that are shared by SSAC and ALAC

---

[1] See: https://www.icann.org/en/system/files/correspondence/odonohue-to-marby-03may19-en.pdf
[2] See: https://www.icann.org/news/blog/icann-meets-with-belgian-data-protection-authority
[3] See: https://gac.icann.org/advice/correspondence/outgoing/GAC%20Chair%20letter%20to%20GNSO%20Council%20Chair%20-%20Next%20Steps%20on%20Key%20Policy%20Issues%20not%20Addressed%20in%20EPDP%20Phase%202.pdf

The SSAC comment on the EPDP Phase 1 Initial Report (SSAC 111[4]) raised numerous concerns that the recommendations would "*fall far short of what the SSAC believes is necessary and possible to address security and stability issues with ICANN's remit*". Similarly, the ALAC also expressed concern about failure to address issues related to distinguishing between legal and natural person registrants and accuracy, among others, in their May 5, 2020 Statement on the Initial Report Addendum[5].

Substantive Failures of EPDP Phase 2 Final Report

In addition to concerns previously stated by the GAC, ALAC, and SSAC, the following failures of the Phase 2 Report cause the BC and the IPC to dissent.

- ***Lack of Centralized Disclosure and Insufficient Mechanisms for Evolution***. After Phase 1, we expected to develop a policy supporting centralized decision making. The inherent inefficiencies and inconsistencies of decentralized decision-making are clear: higher costs to contracted parties, slower disclosure request processing, and greater likelihood of disputes between requestors and disclosers as each contracted party applies its own subjective judgment to each request.

  Nevertheless, in the interest of compromise we agreed to consider (though not accept) a proposed *hybrid model* whereby disclosure decisions would initially be mostly decentralized and manual, but would evolve to automated and centralized processing on the basis of experience gained during the SSAD implementation and increasing legal clarity concerning the interpretation of GDPR requirements.

  Over time we expected that the system, with appropriate safeguards, would automatically provide requested registrant data for settled legitimate purposes, to accredited requestors with their own lawful bases. For example, accredited requestors with reasonable evidence of counterfeit sales or copyright infringement, asserted under penalty of perjury, should rapidly and predictably receive registrant data for relevant domain names. The clarity, consistency, and scalability of such a system would greatly enhance the trust and accountability of the DNS system as access to this data has always done, but is not provided for in the Phase 2 Final Report.

  The Phase 2 Report does not enable ICANN to evolve into its natural role of centralized decision maker. Instead it has the effect of giving the contracted parties undue discretion to individually interpret their obligations under the GDPR and their contracts with ICANN without any requirement for reasonableness, uniformity, or other safeguards. It also fails to provide an adequate mechanism to permit centralization and automation in the future. In doing so it permanently locks in the inefficiencies of decentralized decision-making,

[4] See: https://www.icann.org/en/system/files/files/sac-111-en.pdf
[5] See: https://atlarge.icann.org/advice_statements/13775

such as those resulting in unreasonably long SLAs even for urgent requests related to imminent threats to life or critical infrastructure. (Recommendations 9 and 18)

- ***Failure to Distinguish Between Natural and Legal Persons***. By giving contracted parties the sole discretion to determine whether to differentiate between natural and legal persons, the Phase 2 Report fails to provide clarity regarding access to registrant data for *legal persons* that are not covered by the GDPR. The EPDP team sought and received legal advice from Bird & Bird, the external legal counsel that the EPDP had retained to provide guidance on the GDPR obligations, on how to distinguish between legal and natural person registrants. But it then failed to discuss it, over the objections of the IPC, BC, GAC, SSAC, and ALAC. The continued wholesale redaction of the contact data of legal persons is not required by the GDPR[6], and it erodes trust, accountability and transparency of the DNS. As such, this represents an unacceptable failure of the EPDP. (Recommendation 8)

- ***Failure to Address Accuracy of Data***. The Phase 2 Report fails to address the fundamental issue of accuracy of registrant data, as was agreed by the EPDP in Phase 1, despite the fact that there are adequate tools today to verify the accuracy of registrant data. The inaccuracy of WHOIS data has been problematic for over 20 years. The EPDP Team failed to follow the legal advice it had requested with respect to the interpretation of accuracy requirements under the GDPR. The EPDP Team also failed to follow the advice of the European Commission, which confirmed that data accuracy is not solely in the interest of the data subject. Patently false data is not protected under data privacy laws, and preserving the wholesale redaction of false or fictitious registrant data from the DNS represents another failure of the EPDP, which further erodes trust, accountability and transparency in the DNS. (Conclusion 2)

- ***Inadequate Enforcement Policies***. The Phase 2 Report lacks any contractual accountability for contracted parties to provide data in response to legitimate requests. As mentioned above, the Phase 2 Report fails to adequately provide an objective basis

[6] The comments submitted by Afnic to the Phase 2 Addendum support this view. "*We would like to share our concern with the approach proposing not to distinguish between registrations of legal and natural persons. As many commentators have already pointed out, we believe that this is an over-application of the GDPR. Despite the fact that GDPR does not protect data pertaining to legal persons, we would like to remind ICANN that in its letter dated 11 December 2017, WP29 states the following: 'WP29 wishes to stress that the unlimited publication of personal data of individual domain name holders raises serious concerns regarding the lawfulness of such practice under the current European Data Protection directive (95/46/EC), especially regarding the necessity to have a legitimate purpose and a legal ground for such processing' It appears very clearly that only personal data of individual domain name holders are requested to be protected and undisclosed in the WHOIS. Not distinguishing between legal and natural person is a misinterpretation of European DPA's explicit recommendations on the new legal framework. Afnic as .fr registry operator (ccTLD) has implemented this distinction since 2005 without any operational nor legal issue.*"

and a consistent, predictable and scalable procedure for accredited users to reliably obtain accurate registrant data when there are legal bases and legitimate purposes for requesting and using data, even when the data should not have been hidden in the first place. The Phase 2 Report then fails to empower ICANN to enforce compliance with the weak recommendations made in the Report. A decentralized SSAD has little value if there is no mechanism to ensure compliance with Consensus Policy. Unfortunately, this Report only contemplates enforcement of procedural requirements and does not allow ICANN Compliance to review wrongful denials of legitimate requests. This undermines and delegitimizes the entire policy. (Recommendations 5 and 8)

The result is a Phase 2 Report that recommends a system and policies that are wholly inadequate to meet the stated and agreed goals of an SSAD, including the needs of its users. As a result, the Phase 2 Report fails to maintain the trust, security, and resiliency of the DNS.

In crafting this policy it is essential that the ICANN community support efforts to address growing abuse of domain names that threatens the security, stability and resiliency of the DNS and of the Internet ecosystem more broadly – including the safety and security of its end users. Recently Neustar, a contracted party, addressing the overall growth in internet traffic due to the COVID-19 pandemic and accompanying cyber attacks, reported "*Neustar expected an increase, but we're seeing a dramatic upturn in attacks using virtually every metric that we measure. We have observed an increase in the overall number of attacks as well as in attack severity...*"[7] In addition to noting that it has "*mitigated more than double the number of attacks in Q1 2020 than in Q1 2019*", Neustar reported "*an increase in DNS hijacking, a technique in which DNS settings redirect the user to a website that might look the same on the surface but often contains malware disguised as something useful.*"

Consensus Designations

The IPC and BC remind the GNSO Council and the ICANN Board that the EPDP Phase 2 Final Report defines policy for a single **system** (namely the SSAD). While the consensus call occurs on a recommendation-by-recommendation basis, the recommendations are inherently interrelated and interconnected because of their impact and influence on the SSAD overall. As such, the result of the consensus call should be considered holistically at the system level versus strictly on a per-recommendation basis.

Recommendation #	
#1 Accreditation	Support
#2 Accreditation of Governmental Entities	Support
#3 Criteria and Content of Requests	Support
#4 Acknowledgement of receipt	Support
#5 Response Requirements	Oppose

[7] See: https://www.home.neustar/resources/whitepapers/covid-19-online-traffic-and-attack-data-report

#6 Priority Levels	Oppose
#7 Requestor Purposes	Support
#8 Contracted Party Authorization	Oppose
#9 Automation of SSAD Processing	Oppose
#10 Determining variable SLAs for response times for SSAD	Oppose
#11 SSAD Terms and Conditions	Support
#12 Disclosure Requirements	Support
#13Query Policy	Support
#14 Financial Sustainability	Oppose
#15 Logging	Support
#16 Audits	Support
#17 Reporting Requirements	Support
#18 Review of implementation of policy recommendations concerning SSAD using a GNSO Standing Committee	Oppose
#19 Display of information of affiliated privacy / proxy providers	Support
#20 City Field	Support
#21 Data Retention	Support
#22 Purpose 2	Support

In addition the IPC and BC oppose the language in the following non-recommendation sections:

- Section 1.2 and 2.3 (description of "items not addressed"). We do not support the description of the legal vs. natural outcome.
- Section 3.1 (description of how we got to the "hybrid" model). Our acceptance of the move to a hybrid model was conditioned on the ability to move centralized decisions to the CGM over time using a Mechanism for Evolution that would support that.
- Conclusion - Accuracy (page 60).

Assessing the Overall Value to Requestors

While the EPDP Phase 2 team spent much time and effort in analyzing the financial sustainability of the SSAD itself, we believe it is equally important to analyze the costs and benefits from the users' point of view (i.e. users of the system seeking disclosure of registrant data). This is crucial given that the Phase 2 policy mandates that the requestors pay most if not all costs for the ongoing operation and maintenance of the SSAD and thus we expect the accreditation and request fees to be paid by requestors to be significant.

Further, the SSAD policy as currently defined will have a material impact beyond direct costs on those who have historically relied on WHOIS data. These indirect costs are related to the following:

- **Non-Timely Response**: Because of the failures previously described, the timeframe for responses to disclosure requests will be unacceptably long, impacting the efficiency of processes related to investigating and managing issues of abuse and illegality.

- **Incompleteness**: As there is no longer the ability to perform so-called 'reverse' lookups, it is now harder to identify all of the domains associated with an event or attack.
- **Non-Attribution**: Suppression of reverse lookups interferes with the ability to attribute a criminal or abuse activity with a registrant (actor) in a meaningful response window (if ever). Requestors, especially cyber attack first responders, will rely on proximity factors in lieu of attribution to a greater extent to deploy countermeasures or mitigate attacks.
- **Inaccuracy**: There is no guarantee that data returned will be accurate, nor are there provisions for independent parties to audit registration data for accuracy. Requestors are burdened with the cost of disclosure requests with no certainty of utility or value of the response.
- **Non-Containment**: The inability to perform a timely and complete enumeration of domains associated with a criminal or abuse activity delays mitigation of first response to cyberattacks. Attacks will therefore persist well beyond historical 1-4 hour mitigation objectives. The SLAs as currently defined are insufficient to address issues such as phishing which has a lifetime of hours rather than days, or malware attacks which inflict severe and direct costs or losses upon their victims.
- **Unpredictability**: A decentralized and distributed disclosure model will result in an unpredictable and unreliable system for access and disclosure. This blocks efforts by requestors seeking disclosures from multiple contracted parties for large numbers of domains associated with a single cybercrime or abuse activity.

We have always acknowledged the need to pay accreditation fees in order to use the SSAD. However, it is clear that the value and benefits of the SSAD, as defined by the Phase 2 Final Report, do not come close to justifying the costs (direct and indirect) of using the SSAD.

Conclusion

When the ICANN Board adopted the Temporary Specification in May 2018, it noted, "*the Board's actions are expected to have an immediate impact on the continued security, stability or resiliency of the DNS, as it will assist in maintaining WHOIS to the greatest extent possible while the community works to develop a consensus policy.*"[8] At the November 2019 ICANN66 Montreal meeting, the ICANN Board and CEO reiterated in the open forum the importance of scalable access to registrant data to ensure the safety and security of the Internet and its users. The results of over two years of intense work by the EPDP team amount to little more than affirmation of the [pre-EPDP] status quo: the elements of WHOIS data necessary to identify the owners and users of domain names are largely inaccessible to individuals and entities that serve legitimate public and private interests.

[8] See: https://www.icann.org/resources/board-material/resolutions-2018-05-17-en

For the reasons stated above, our Board-approved missions and purposes compel us to dissent from the set of policy recommendations set forth in the Phase 2 Final Report.

Despite the IPC and BC's best intentions, the EPDP experiment has failed. It has proven incapable of handling a purely legal issue created by the GDPR. Regulators and legislators should note that the ICANN multi-stakeholder model has failed the needs of consumer protection, cybersecurity, and law enforcement. As a result, there is a need for clear regulatory guidance for the GDPR, and to pursue alternative legal and regulatory approaches.

About the BC and IPC

The mission of the Commercial and Business Users Constituency (BC) as approved by the ICANN Board is "*to ensure that ICANN is accountable and transparent in the performance of its functions and that its policy positions are consistent with the development of an Internet which...promotes user confidence in online communications and business interactions…*"

The purpose of the Intellectual Property Constituency (IPC) as approved by the ICANN Board is to "*represent the views and interests of owners of intellectual property worldwide with particular emphasis on trademark, copyright, and related intellectual property rights and their effect and interaction with Domain Name Systems (DNS), and to ensure that these views, including minority views, are reflected in the recommendations made by the GNSO Council to the ICANN Board.*"