Non-Commercial Stakeholders Group
Representing the interests and concerns of
non-commercial Internet users in domain name policy

9 April 2018

To: Mr. Cherine Chalaby
Mr. Göran Marby

CC: Mr. John Jeffrey
Mr. Akram Atallah
Mr. Cyrus Namazi
GDPR@icann.org

Comments of the Non-Commercial Stakeholders Group on the *Draft IPC/BC Purpose Statement* Published on 27 March 2018

During ICANN 61 in San Juan, representatives of the Intellectual Property Constituency and Business Constituency shared a draft *Purpose Statement for the Collection and Processing of WHOIS Data* and draft accreditation model for access to domain name registrant data.[1]These materials were not circulated to the Non-Commercial Stakeholders Group (NCSG) prior to presentation to the community despite sharing the same House in ICANN governance structure.

Accordingly, what we have before us is not a "community statement," in contrast to how it was presented in the Public Forum in San Juan, and not a properly labeled document. We therefore ask for the IPC and BC to properly identify these works for future discussion as the ***IPC/BC*** *Purpose Statement* and the ***IPC/BC*** *Draft Accreditation & Access Model For Non-Public Whois Data*.

We will comment in the future on the *IPC/BC Draft Accreditation & Access Model For Non-Public Whois Data.* The goal this comment is to rapidly share our deep concerns about *IPC/BC Purpose Statement for the Collection and Processing of WHOIS Data.*

A. This IPC/BC Purpose Statement Misses the Whole Point of the Exercise, Namely Protecting a Registrant's Fundamental Right to Privacy

As a Community, we have undertaken the review of domain name registration data because the European Union's General Data Protection Regulation (GDPR) provides harmonized data protection rules with enhanced enforcement, in line with the European Charter of Fundamental Rights which in Article 8 provides that the protection of personal data is a fundamental right. Real obligations, responsibilities, and fines face those parties, of which ICANN is among them, who collect and process domain name registrant data as of 25 May 2018. Yet, the goal of our work -- protecting the fundamental rights of domain name registrants from the dangers to which they might be subject should their names, address, phone numbers,

[1] ***IPC/BC*** Draft Accreditation & Access Model For Non-Public Whois Data, March 27, 2018, Version 1.3, *http://www.ipconstituency.org/assets/docs/WHOIS%20Access%20Accreditation%20Process%201.3[1].pdf; see Annex A: [**IPC/BC**] Purpose Statement for the Collection and Processing of WHOIS Data, p. 15.*

and email addresses be exposed -- remains buried and undiscussed in this newest version of the so-called "community materials."

Simply put, the *IPC/BC Draft Accreditation & Access Model For Non-Public Whois Data* and *IPC/BC Purpose Statement for the Collection and Processing of WHOIS Data* ("IPC/BC Purpose Statement") are not compliant with the GDPR. They ignore the fundamental rights of data subjects -- domain name registrants -- and put the users of the data ahead of the data subjects, in violation of the GDPR.

We would note that that the *IPC/BC Purpose Statement* is not alone in ignoring the fundamental right to privacy of domain name registrants. The final report of the Expert Working Group on gTLD Registration Directory Services suffered from the same shortcomings. The EWG presented a long list of *existing uses* of domain name data, but failed to balance those uses against the *fundamental right to privacy* which domain name registrants inherently hold. This fundamental flaw was pointed out in a timely dissent filed by the EWG's only data protection expert, Stephanie Perrin, a drafter of the Canadian data protection statute.[2] The *IPC/BC Purpose Statement* relies heavily on this EWG Report and suffers from its shortcomings.

B. NCSG Represents Those Protected by the GDPR, Including Human Rights Groups

The Non-Commercial Stakeholders Group is in a special position to raise concerns. We promote non-commercial interests in policy development and represent more than 500 nonprofit organisations and individuals who wish to advance non-commercial policy objectives at ICANN. We are proud to have human rights organizations, LGBTQ groups, representatives of religious groups and an array of minority ethnic, political, cultural groups, along with individual users of the Domain Name System, among our members. We have shared our concern for nearly two decades that ICANN's publication of WHOIS data has led to spamming, harassment, stalking, and threats of imprisonment to domain name registrants, and provided examples. We have emphatically noted the problem that speech -- completely legal in one jurisdiction (such as where the domain name is registered and registrant resides) -- is deemed illegal, criminal, blasphemous, and/or treasonous in another jurisdiction (such as where that registrant is from and/or where his/her family may still reside). We know firsthand who the GDPR seeks to protect, and why, and join the ICANN Community in recognizing that more than 120 countries around the world recognize privacy as a fundamental human right for very good reasons.

Clearly, the fundamental right of domain name registrants to privacy is a concept which must now be embraced by any GDPR-related materials created by ICANN -- including our future "community purpose statement" -- if we are to legally collect and process domain name registration data. Not doing so will expose those who collect and process the data -- registries, registrars, and ICANN org -- to enormous liability and fines; not doing so will rob individuals and groups of individuals of their fundamental right to privacy and expose them to enormous risks, including their freedom.

[2] *See, e.g., ICANN Suppresses a Privacy Advocate's Dissent,* www.internetgovernance.org/2014/06/07/icann-suppresses-a-privacy-advocates-dissent/

C. *Draft IPC/BC Purpose Statement Does Not Meet with the Requirements of Law*

NCSG offers this point-by-point critique of the *IPC/BC Purpose Statement* to help advance our work together. We draw from "lessons learned" in our high level session at ICANN 58 in Copenhagen with Data Protection Commissioners, from the Hamilton Advokatbyrå law firm memos to ICANN and from the many GDPR compliance classes being offered globally. We offer this critique in a constructive vein -- to achieve the goal of an interim "community purpose statement" of the type urged upon us by Göran Marby, John Jeffrey, Cyrus Namazi and Akram Atallah at ICANN 61 in San Juan.

(i) Why We Collect Domain Name Registration Data

Under the GDPR, ICANN's purpose statement for collecting and processing registrant data must fall within the limited scope and mission of ICANN. Personal and sensitive data may only be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes" (Article 5, GDPR).

What falls within ICANN's scope and mission according to our new bylaws? ICANN is an organization dedicated to the safety and security of the Internet. We have a limited mission, and content is expressly outside of it. See Article 1, Sec.1.1 of the Bylaws. Considering ICANN's limited mission, the main "purposes for processing" domain name registrant data are:

(a) For administrative actions supporting a registrant, namely: "the invoicing, support and other administrative actions in relation to registered domain names;" and
(b) For recovery purposes, namely "safeguarding the rights of registrants, for instance by retention of the data in escrow with escrow agents, for recovery in the event of e.g., a distressed registrar or registry or failure by a registrar or registry to fulfill its obligations." (Hamilton Memo #3, p. 4)[3]

These are the clear and concrete purposes for the collection and processing of registrant data that would be compliant with the GDPR and consistent with the scope and mission of ICANN. This is what should be reflected on the first page of an ICANN Community Purpose Statement, and we note that it is not.

(ii) Who Else Wants a Registrant's Domain Name Registration Data

As the *Draft IPC/BC Purpose Statement* shows, many people and groups want to use domain name registration data for secondary purposes. The key to evaluating their requests under the GDPR is not who wants the data, but whether their request for the data is properly balanced against the fundamental privacy rights of the data subject, the registrant.

[3] ***gTLD Registration Directory Services and the GDPR - Part 3,*** to ICANN from Thomas Nygren and Pontus Stenbeck, Hamilton Advokatbyrå, 16 October 2017 ("Hamilton Memo #3), https://www.icann.org/en/system/files/files/gdpr-memorandum-part3-21dec17-en.pdf

Hamilton Memo #3 notes that even in the most persuasive secondary use of the data, namely law enforcement seeking to investigate a crime, there are limits to what can be provided and guidance on who oversees the law enforcement request and balances the rights of the registrants under the GDPR:

> "Article 6.1(f) GDPR can most likely not be used to provide all law enforcement agencies unfiltered access to all Whois data but such access would likely have to be assessed in light of Article 6.1(f) GDPR, with the appropriate balancing of interests, in each case."[4] (Hamilton Memo #3, p. 8)

> This balancing also applies to those processing domain name registration data for the investigation of fraud, consumer deception and intellectual property infringement. Under Article 6.1(f) of the GDPR, the interests and needs of these groups must be weighed against, and override, the interests or fundamental rights and freedoms of the data subject, e.g, the registrants. (Hamilton Memo, p. 9)

This is a fundamental change that we must recognize, and that is neither understood nor acknowledged in the materials we are evaluating.

(iii) NCSG revisions to the ten proposed purposes of the *IPC/BC Purpose Statement*

In evaluating the *IPC/BC Purpose Statement*, in light of ICANN's limited technical mission, we offer some revisions to the ten proposed purposes:

1. Deletion of #1: "*Providing access to accurate, reliable and uniform registration data in connection with the legitimate interests of the registrar and WHOIS system stakeholders"*

This purpose statement is redundant, and unfortunately, circular. It says that ICANN must provide registrant data to anyone who wants wants it -- to any "WHOIS system stakeholder," which is, frankly, everyone. There is no way that such a broad statement is even a) a purpose statement at all, or b) even a reasonable outline of how to properly provide registrant data for secondary purposes on specially balanced provisions that the GDPR requires (as discussed above). This statement is a non-starter and a hold-out from the old WHOIS days.

The NCSG asks that the following language be inserted instead into our community purpose statement would be: ***Collect and process domain name registration data in a matter designed to protect the domain name registrant's fundamental right to privacy, and minimized to provide for administrative processing***

[4] Further, the Court of Justice of the European Union (CJEU), charged with ensuring that EU law is interpreted and applied uniformly in every EU member state, determined that: "access to retained data by competent law enforcement agencies as a general rule must, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those law enforcement agencies submitted, *inter alia,* within the framework of procedures for the prevention, detection or prosecution of crime. Although the referenced CJEU cases, in part, concerned different kinds of data for different purposes than what is the case in relation to the Whois services, the CJEU clearly established that disclosure to law enforcement agencies for crime fighting purposes should primarily be tried and decided by competent courts." (Hamilton Memo #3, p. 8)

of the data and recovery purposes that safeguard the interests of the registrant in the event of registrar or registry failure.

2. Deletion of #2: "*Enabling a dependable mechanism for identifying and contacting the registrant."*

This is not a purpose statement consistent with the principles of the GDPR. If a fundamental right to privacy exists, and the GDPR of course indicates that it does, then identifying and contacting the registrant of a domain name cannot be the primary purpose of the system. In order to achieve compliance with data protection laws, .NL (managed by Stichting Internet Domeinregistratie Nederland, SIDN) has already withdrawn public WHOIS data. There is expressly no easy way to identify and contact the registrant; all requests for such data are legally balanced against the registrant's fundamental right to privacy.

As Hamilton Memo #3 notes, contacting the registrant need not be done by identifying them. The many requests that a registrant may receive seeking to acquire their a domain name (to which a registrant need not respond) can be sent to them via a webform or one-time email address; ditto for allegations of trademark and copyright illegality (to which a registrant also has no legal obligation to respond). **Identification of a domain name registrant is, of course, the most dangerous part of the process and brings potential dangers to the individual, their family and minority groups of which they may be a part** – *the very type of persecution the GDPR is designed to prevent.*

The NCSG asks that the following language be inserted instead into our community purpose statement: ***Request gTLD registries and registrars provide a way to allow the public to contact registrants, without disclosing the registrant's identity.***

3. Deletion of #3: "*Enabling the publication of points of contact administering a domain name*."

This is not a legitimate purpose. The "publication" of points of contact administering a domain name reveals the name, location, phone number, and other personal information of individuals, including those in organizations. Such information is expressly protected by the GDPR.

If we are adopting "privacy by design," which the GDPR requires and which technologies and timing expressly enable, we can get this right. We collect and process no more data than is needed to facilitate administrative contact with the registrant, and provide that data only as required by law. The ECO model provides an excellent analysis of what contact points are needed for that process. Certainly "publication" -- as in the express provision of that information to the "public," e.g., through directories -- as stated in this #3 point, is expressly barred by the GDPR, as the Hamilton memo and the Article 29 Working Party have shared.

The NCSG asks that the following language be inserted instead into our community purpose statement:

Collect only the registrant data needed for domain name administration.

4. Deletion of #4: "*Providing reasonably accurate and up-to-date information about the points of contact administering a domain name."*

This is hardly a "purpose statement" as it does not provide guidance on how registrant data should be collected and processed. Of course, registrants should provide necessary, appropriate, and accurate data, as discussed above, and registrants must have the opportunity to easily correct that data as it changes over time, e.g. moving one's house or apartment. This is required by the GDPR and likely does not need express inclusion or further discussion.

5. Deletion of #5: "*Providing access to registrant, administrative or technical contact for a domain name to address issues involving domain name registrations, including but not limited to: consumer protection, investigation of cybercrime, DNS abuse and intellectual property protection."*

The NCSG considers this statement to be overly broad and inconsistent with the principles of "privacy by data" that the GDPR requires. This statement embraces all of the ancient domain name contact fields, including fields such as one's facsimile number, regardless of their relevance in our contemporary society. In addition, this statement fails to even breathe a mention of the primary purpose of the GDPR, namely protecting the privacy of the domain name registrant, including from overly broad searches by their own governments and law enforcement officials (and those of other countries).

The Hamilton memo's legal analysis makes very clear that mere requests from consumer protection professionals, from investigators of cybercrime and DNS abuse, and from IP attorneys "does not automatically qualify as a legal ground [for access to the registrant data]":

> *"If a registrar receives a request from the public to disclose additional data, the registrar must then, in each individual case, assess whether legal ground to disclose such data exists. In practice, the registrar would have to perform an assessment of whether sufficient legitimate interest exists in accordance with Article 6.1(f) GDPR and whether or not the interests or fundamental rights and freedoms of the registrant override such interest."* (Hamilton Memo #3, pp. 10-11)

Even having "automatically qualified parties," as some in the list of proposed #5 might constitute:

> *"Would face similar challenges. Having such automatically qualified parties requires that it must be possible to, on a general basis, <u>determine that a certain type of party always is qualified to access certain data based on Article 6.1(f) GDPR (or any other legal ground set out in the Article 6.1 GDPR)... This type of generalized assessment is however, in our opinion, very difficult to apply in order to automatically qualify, for instance, intellectual property lawyers or similar categories to assess data that is not permitted to publish publicly."</u>* (Hamilton Memo #3, p. 11) [emphasis added]

The NCSG asks that the following language be inserted instead into our community purpose statement: ***Provide balanced and proportionate access to appropriate and limited registrant data for consumer protection, investigation of cybercrime, DNS abuse, and intellectual property protection consistent with***

the protection of the fundamental rights of the registrant to privacy and assessment and balancing of interests of the requestor and the registrant rights as required by both letter and spirit of law.

6. Deletion of #6: "*Providing registrant, administrative or technical providers for a domain name to address appropriate law enforcement needs."*

The NCSG understands the deep desire for the data of domain name registrants to be used in this manner. We also understand, perhaps better than many within the ICANN community, the direct harm which can come to domain name registrants and/or their friends, families, and communities if they are identified by law enforcement from a jurisdiction in which, for example, they are not residing but to which their religious views, sexual orientation or gender identity, pro-democracy perspective, pro-women and girl's education views, or anti-leader views may be viewed as illegal, immoral, treasonous, blasphemous, problematic, and/or criminal.

These are human rights issues that individuals and organizations face on a daily basis around the world. The GDPR provides express and explicit protection for the fundamental privacy rights of the registrant, and appropriate access for law enforcement. The Hamilton memo shares that law enforcement requests are properly "subject to approval from relevant courts" who will then determine if any distinction should be made between EU and non-EU law enforcement agencies when assessing whether to provide access to the data." (Hamilton memo #3, p.8) We have a legal obligation to comply with the law, which this current statement does not.

The NCSG asks that the following language be inserted instead into our community purpose statement:

> ***Provide access to appropriate registrant data for law enforcement needs consistent with the protection of the fundamental human rights of the registrant and assessing and balancing of interests of the requestor and the registrant rights as required by law.***

7. Deletion of #7: "*Facilitating the provision of zone files for gTLDs to Internet users."*

Unfortunately, this sentence does not even fall close to the mark of what is required of a "purpose statement," or subsection thereof, under law. The protection of the fundamental right to privacy hardly includes the bulk access to the millions of gTLD domain names by any "Internet user" who may so choose. This is a non-starter.

8. Keep #8: "*Providing mechanisms for safeguarding registrants' registration data in the event of a business or technical failure, or other unavailability of a registrar or registry."*

The NCSG understands the intent behind this purpose statement, however we believe the Hamilton memo stated this purpose in a clearer and more narrowly tailored way. The NCSG asks that the following language be inserted instead into our community purpose statement:

> ***For recovery purposes, "safeguarding the rights of registrants, for instance by retention of the data in escrow with escrow agents, for recovery in the event of e.g., a distressed registrar or failure by a registrar or registry to fulfill its obligations." (Hamilton memo #3, p. 4)***

9. Replace #9 "*Coordinating dispute resolution services for certain disputes concerning domain names."* with:

NCSG advises that the following statement be inserted instead:

> ***Coordinating dispute resolution services for certain disputes concerning domain names consistent with the fundamental rights of the registrant and the goals of rapid domain name dispute resolution.***

10. Discuss further #10: "*Ensuring that ICANN fulfills its oversight responsibilities and preserves the stable and secure operation of the Internet's unique identifier systems through a minimum, addressing contractual compliance functions (including complaints submitted by registries, registrars, registrants, and other Internet users) as well as other necessary oversight functions, such as reporting, policy development, and implementation."*

This is a bit of the "kitchen sink" approach and we doubt that there is anyone or anything under this umbrella, as written, would be denied access to registrant data. There is absolutely no protection for the fundamental privacy rights of registrants, and support for anything people and organizations complaining to ICANN might seek. Clearly, that is not a legal balancing of interests under law. We note further that the Hamilton law firm has cautioned us:

> *"Where the data controller is not a party to the contract with the registrant, which is the case for ICANN and the registries, performance of a contract in accordance with Article 6.1(b) GDPR cannot be used as legal ground for processing for administrative actions." (Hamilton #3, p. 6)*

The NCSG believes it would be better to stick with the administrative actions we know and understand in our purpose statement:

> ***For administrative actions supporting a registrant, namely: "the invoicing, support and other administrative actions in relation to registered domain names."***

D. Conclusion

We note, in closing, that ICANN is not an intellectual property law firm, a brand protection firm, a law enforcement agency, nor any form of government regulatory agency. **In 1998 and again in 2016, we - the ICANN community - rejected expansions of ICANN's mission.** Our "purpose statement" must therefore be limited to what we do together in ICANN.

Further, the vast majority of potential users of the domain name registration data, shared on pages 17 to 23 of the *IPC/BC* Draft Accreditation & Access Model For Non-Public Whois Data, March 27, 2018, Version 1.3, must drop away to be consistent with the discussion of ICANN's limited scope above, and the clear requirements of the GDPR. Further, NCSG notes that the Draft Accreditation Model fails to mention the upcoming Article 29 Working Party guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679. Clearly the fact that the Article 29 WP has stated it will issue an annex which provides a toolbox for accreditation criteria is a positive and useful sign. NCSG advises that much time will be saved

if we put a halt to our discussion of accreditation models and wait for the legal authorities to issue the guidelines we should follow.

We look forward to the discussion ahead, but note that the law in which we together must comply is neither optional nor discretionary. Following the GDPR is not a matter for community consensus for ICANN, but a matter of community compliance.

Respectfully shared,
Farzanah Badiei, Chair, and The Non-Commercial Stakeholders Group