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

5 March 2018

To: Isabelle Falque-Pierrotin, Chairwoman, Article 29 Working Party
Andrea Jelinek, incoming Chairwoman, Article 29 Working Party

cc: Cherine Chalaby, Chair, ICANN Board of Directors
Göran Marby, ICANN Chief Executive Officer

Re: ICANN's non-compliance with European data protection law

Dear Mme. Falque-Pierrotin and Mme. Jelinek,

I am writing to you on behalf of the Noncommercial Stakeholders Group (NCSG) at ICANN. The NCSG represents the interests of non-commercial domain name registrants in the formulation of Domain Name System policy under the auspices of ICANN's Generic Names Supporting Organization (GNSO). We are proud to have individual and organisational members in over 160 countries, and enjoy a thought leadership position in the domain name industry, particularly on matters to do with privacy and data protection, and free speech. Since 1999, our organization has facilitated global academic and civil society engagement in support of ICANN's mission, stimulating an informed citizenry and building their understanding of relevant DNS policy issues, notably the need for ICANN to comply with privacy and data protection legislation.

In this respect, we have engaged with members of the Article 29 Working Party over many years, and appreciate very much your support in attempting to influence ICANN's WHOIS (Registration Directory Service, RDS) policy. Unfortunately, these efforts have born little fruit to date, but it appears that the reality of increased fines and enforcement action which come into effect with the enforcement of the European Union's General Data Protection Regulation (GDPR) in May 2018 has prompted ICANN to examine its practices afresh. They have released an interim model for their contracted parties, the registrars and registries, to comply with pending further policy development.

We are aware that the ICANN corporation, along with other interest groups within the multistakeholder community which set Domain Name System policy, have written to you recently in relation to the impact of the GDPR on WHOIS. We also understand that ICANN's Chief Executive Officer Goran Marby has encouraged all stakeholder groups to make contact with you to seek guidance and engage in a dialogue. We are well aware of the many communications between the Article 29 Working Party and ICANN since the publication of your Opinion on WHOIS in 2003, and we understand that you must be extremely busy at the moment and do not need us to restate the many points you have made over the years. We are also strongly supportive of the recent working document from the International Working Group on Data Protection in Telecommunications, and

don't wish to reiterate the points made in that document as well. However, with apologies for the late arrival of this representation of our views, we do think it important that you hear from civil society on certain aspects of this subject.

We do not have the funds to lobby, attend conferences, or send representatives to Brussels, but please rest assured we have an abiding interest in this topic and are active on many committees at ICANN which are addressing policy aspects of the Registration Data Services (RDS).

We would like our colleagues in government and the private sector to embrace the spirit of the GDPR, and to understand how data protection is rooted in the Charter of Fundamental Rights of the European Union. At the moment, the goal of many stakeholders at ICANN is to maintain registration data services as close to the status quo as possible, and it has been from that angle that the ICANN corporation has sought to comply with the GDPR. The corporation seeks not to comply with the spirit of the GDPR but only with the very letter of the law, and many discussions have centred around how to not "over comply" with this regulation. This is disappointing, in 2018.

It is the view of the NCSG that the status quo has been illegal under data protection law since the birth of ICANN in 1998, that the status quo is not worth preserving, and that registration data requirements need to be rethought from scratch in a holistic manner, not merely focusing on the publication instrument of WHOIS. It is most unfortunate that the publication of personal data over so many years, and ICANN's encouragement of the bulk capture of data for re-publication by value-added services[1] have enabled users and scrapers of the data to claim that all these subsequent uses of registration data by third parties are essential to the security and stability of the Internet. Not only is this not the case, it ignores the very real risk to individuals of publishing their data (which includes the registrant's name, email address, phone number, and home address, among other fields) for the entire world and all its bots to see and capture.

The NCSG has over the years compiled many examples of harassment, physical endangerment, religious persecution, and commercial bullying arising from the openness of the WHOIS data. The issues came up recently when a policy development process for the Accreditation Issues of Privacy/Proxy Service Providers was established and public comments were sought. We received many examples of recent threats to privacy and

[1] For examples of such value-added services, please see Domain Tools (www.domaintools.com), which harvests domain name registration records and sells access to these records for USD 995/year, and a myriad of other tools (https://www.dataprovider.com/products/ownership/ ; whois.com ; who.is (who charge registrants USD 10 to have their records removed;
https://tool.domains/ ; https://www.domainiq.com/ ; or the following articles

https://domainnamewire.com/2016/01/08/another-disturbing-whois-data-service/
https://domainnamewire.com/2015/06/29/spamming-owners-of-newly-registered-domain-names/

safety, including harassment of women that followed the famous Gamergate debacle[2], unsolicited advertising and fraudulent marketing. ICANN is neither a business regulator nor is it a consumer protection agency. The RDS is neither a substitute, replacement, nor proxy for the work of governments in protecting consumers. Governments can and do mandate what data must be made available on the websites of entities selling goods to the general public. Governments can and do educate consumers to deal only with those entities whom they know online and that have complied with the legal requirements of disclosure and presentation.

We hope that pressure will be put on ICANN to remain within its limited remit, and to restrict its data collection, use, and disclosure practices to only those which are necessary for the registration of a domain name, rather than serving the potential data desires of a myriad of third party stakeholders.

Here are a few of the issues that are important to us.

Recommendations

Purpose of the Processing of Registrant Data

As discussed above, ICANN is trying to retain as much of the status quo as it can. Many stakeholders are trying to do this by claiming that the many uses of registrant data that have sprung up over the past 20 years, including the analysis and enrichment of this data by value added services, are part of the purpose of processing which ICANN oversees. We disagree. The purpose of processing registrant data is to register a domain name and ensure its effective functioning in the DNS. Certainly the data can be provided to law enforcement following due process. Similarly it can be provided to intellectual property holders who can show evidence of abuse. This does not make law enforcement, or intellectual property and trademark enforcement a purpose of data processing at ICANN.

Status of the registrant, natural person or legal person

We recognize that the remit of your group is the protection of personal data, and therefore you have not advanced arguments for the protection of legal persons. The NCSG has long argued for the protection of legal persons too, because there are many human rights and data protection issues associated with small home-based entrepreneurs, journalists, religious and political associations, and human rights organizations having their physical location accessible through the RDS. Contact details which are released in WHOIS have

[2] For an explanation of Gamergate, see http://gawker.com/what-is-gamergate-and-why-an-explainer-for-non-geeks-1642909080. The kind of harassment and cyberbullying that has arisen in recent years has made numerous groups and individuals much more aware of the risks associated with any personal data being released in a public directory, particularly in the light of increasingly accurate and effective mapping and geolocation services.

led to the harassment of staff, persecution of organizations who engage in free expression (particularly political speech), and have resulted in death threats because of the activities of some members of groups. There have been documented instances of the WHOIS being used to dox or swat domain name registrants; particularly female registrants. We believe there is also an employee privacy issue, even in those states and territories where there is no data protection law. At the end of the day, data stored in WHOIS can and has led to harassment, stalking, physical harm, psychological harm, and unnecessary threats to ideas and communications. Accordingly, we believe all domain name registrants should be protected from these abuses.

A further question arises as to the efficacy of making a distinction between a natural person or a legal person. If an individual decides to register a half dozen names they happen to think of, they may not have decided what they would use them for. It is not the case that a domain name equals a website, nor that a website is engaged in commercial activity. Obviously big businesses such as Facebook and Apple have a strong interest in releasing a great deal of information about themselves, to assist in the prompt investigation and takedown of any possible fraudsters who have registered their brands, and we generally agree that if they wish to have many data fields visible to ensure that end users are not duped into participating in their own identity theft or purchasing fake goods, they should be able to do so. The same is not true of small businesses; we argue that the reverse risk scenario is true, they are more likely to experience fraud if their address, phone numbers, and employee contacts are published. There are many small entrepreneurs, particularly women, who can make excellent use of the Internet to promote their home businesses. Sole proprietors should not be forced by ICANN to release their home address, phone numbers, and email. E-commerce standards for transparency about web presence should be set by local law, not by ICANN.

Publication of WHOIS Data and Tiered Access

Several of the interim models that ICANN and its stakeholders are proposing, including the draft released on February 28th utilize tiered access. While there is a range of views in the NCSG about publishing any personal data in the WHOIS or its replacement, we are united in the belief that tiered access, if it is adopted, must have an extremely rigorous process to accredit those who wish access to personal data.

Law enforcement must follow proper legal procedures, and obtain whatever kind of court order or subpoena is required by local law. Investigations across national boundaries should follow the procedures of the Budapest Convention. If law enforcement is experiencing difficulties with Mutual Legal Assistance Treaties and the procedures thereunder, they must deal with them at the government level and not ask ICANN to create streamlined procedures for them in a private sector information clearinghouse.

Similarly, due process must be followed before access to registration data is given to a lawyer for the purposes of investigating alleged trademark abuse. Proposed models which see lawyers and paralegals automatically accredited to access a tiered-access system are improper. The mere proof of being a legal professional and the mere allegation of a legal

problem is never enough to cause a defendant to lose his or her rights, privileges and protections. Societies with lawyers protect against their abuses. For example, to attain the identity of a "John Doe" (an unidentified person) in offline applications, lawyers may not merely make an allegation of wrongdoing or breach, he or she must file a lawsuit, show a justified legal claim, and affirm they will not misuse the identity when disclosed. If the conditions are met, and the disclosure made, the attorney's actions are monitored by a judge or magistrate for the protection of the John Doe. Due process rules ensure that all parties - large and small, represented and not - have the time and notice needed to prepare and ready themselves for legal steps.

For these reasons we similarly do not approve of self-certification. The 'honor system' would merely turn the existing system into one where privileged actors would get beyond the first tier and continue the all-you-can-eat approach to data access. Registrars and registries bear the economic and work burdens of any access restrictions, so a dialogue with them about how to facilitate legitimate access to data for limited and appropriate purposes should commence as soon as possible. To the best of our knowledge, there is no public discussion at ICANN at the moment about how to authenticate requestors and to ascertain their legitimate purposes, and we believe this is clearly required under data protection law. The February 28th proposal to have the Government Advisory Committee accredit law enforcement agencies and third parties such as cybercrime fighters and intellectual property enforcement agents prompts skepticism among our members, given the long history of that group's pressure on ICANN to maintain an open WHOIS, and the lack of resources they dedicate to actual policy development at ICANN. This will not be a simple task.

Fighting fraud, trademark abuse, and cybercrime

We recognize that fighting cybercrime is a job that has been largely relegated to the private sector. There are many competent organizations who are working in this field, but their access to registrant data has thus far not been subject to any kind of regulation or standards, rather it works in a network of trust. This does not scale, with the number of Internet users today and the need for a global approach to fighting crime, and therefore strict standards of professional conduct, with expected privacy and security protocols, need to be developed. Some of our members are attempting to promote the development of such standards and protocols, because we do not believe that self-accreditation, or any kind of accreditation that ICANN might develop, will be in the best interests of domain name registrants and Internet end-users.

Privacy policy for ICANN

We have long argued that ICANN needs a privacy policy, not just for its own internal practices but for every aspect of its control of registrant data. It is very clear that ICANN has no privacy policy; the data collection, use, and disclosure of registrant data is set in the Registrars Accreditation Agreement, and this is not a consensus policy document, it is a bilateral negotiation between the registrars and ICANN, where ICANN holds the

dominant power because the registrars cannot do business in registering domain names unless ICANN accredits them. It is very clear that ICANN is the data controller here, because it sets the requirements for every aspect of data use in this agreement.

The WHOIS Conflicts with Law Policy, which is often pointed to as the policy governing WHOIS data, is not a policy in as much as it is a procedure. If a registrar can manage to prove to ICANN that it is violating local law by adhering to its contractual obligations, it can obtain waivers for publication of personal data in the WHOIS, or data retention requirements. We think this is non-sensical in a world with over 120 data protection laws. It is anti-competitive because actors who obey the law have a work threshold and expense that scofflaws do not, and it fails to recognize the other aspects of data use that are problematic from a data protection perspective. We also note that the procedure is unworkable in practice, as evidenced by the fact that no one successfully utilized it for over 10 years. A comprehensive privacy policy is required to deal with issues such as collection, use, procedures for disclosure, record-keeping in terms of those disclosures, access, correction and erasure rights, meaningful transparency surrounding data practices, rights of complaint to an independent authority, and breach disclosure provisions.

We believe that such a policy could become the foundation of binding corporate rules that would go a long way to guaranteeing privacy rights.

Summary Comments on the February 28 Model for GDPR Compliance

The proposed interim model is available here https://www.icann.org/en/system/files/files/proposed-interim-model-gdpr-compliance-summary-description-28feb18-en.pdf. Our preliminary comments include:

- The goal of this policy is to retain as much of the status quo as possible, not respect registrant rights.
- Respect for data protection law outside the EEA remains optional.
- "Robust collection" is maintained. This is over-collection.
- Tiered access will be managed through an accreditation scheme developed by the Government Advisory Committee (GAC). We do not believe this would effectively protect registrant rights, based on 20 years of experience with the GAC on WHOIS debates.
- The analysis of this document rests on the foundation of the current system. We believe a completely de novo approach is required.
- "The legal justification for collection, use, and publication of the WHOIS data will be based on legitimate interests of the controllers, data subjects, and third parties, which will be discussed on a detailed basis in an analysis that will accompany the final version of the model"(p. 8). We do not believe that the interests of third parties constitute a valid legal justification for the collection, use, publication and disclosure of registrant data. There is at ICANN a persistent conflation of the interests of third party stakeholders in obtaining detailed information about registrants, and the purpose of ICANN. We draw your attention to this persistent conflation. The document

discusses the legal basis for processing which it intends to develop in Section 10, p. 9. It is the view of the NCSG that if broad purposes encompassing law enforcement, trust on the Internet, and consumer protection are embraced in this development of purposes and justified as described, we will simply have the current WHOIS behind a wall where dominant actors will continue to freely access unlimited data. The expense of this wall will be passed on to registrants, further discouraging the participation of individuals in the DNS. We will of course be arguing against such an approach, but we wished to draw your attention to this matter, especially in the light of their summary statement "This analysis will take into consideration that the WHOIS service is provided pursuing various public interests, as confirmed by the European Commission, which may constitute relevant legitimate interests pursuant to Art. 6 (1) (f) GDPR."

Registrant data issues beyond WHOIS

Certainly the Article 29 Working Party has raised other issues concerning registrant data over the years; Jacob Kohnstamm wrote to ICANN several times concerning the provisions of the proposed 2013 Registrars Accreditation Agreement, the waiver requirements, and the illegal nature of the data retention requirements. Those issues persist today, and the recent thick WHOIS policy now requires the transfer of a great deal of registrant data outside of Europe and into foreign registries, notably Verisign of Virginia, United States, which remains the largest registry in the world. This policy has been put on hold at the moment, and it is our view that until a convincing rationale for personal data being exported to foreign registries can be advanced, the data should remain with the registrars.

One of the recent contributions to the discussion of GDPR compliance is a comprehensive Playbook prepared by the ECO Internet Association, a consortium of registrars and registries. It explores some of the issues that are of great concern from a privacy perspective, but are not part of the compliance models being proposed, such as access to zone files and re-processing of that personal data. We would encourage the Article 29 Working Party, if they are investigating ICANN's practices, to examine this publication, because it is the most comprehensive discussion of the privacy issues that has been tabled during the GDPR compliance activities which are proceeding at the moment (see the second chart, approx. page 2, model CM3 https://www.icann.org/resources/pages/gdpr-legal-analysis-2017-11-17-en).

We respectfully submit that the status quo cannot continue, as it involves too much disclosure of information with too little due process and even less protection for the domain name registrant. The best alternative is to limit the data in the WHOIS – provide a mechanism for contacting the registrant for technical questions, delete physical location data (which can still be found through the registrar subject to the appropriate jurisdictional protections for the registrant).

We hope our comments are useful and we would be happy to answer any questions you may have. Thank you very for your continuing interest in ICANN, and the protection of registrant rights.

Yours sincerely,

Dr. Farzaneh Badiei
Chair, Noncommercial Stakeholders Group

About the NCSG

The only place within ICANN that is specifically reserved for the advancement of non-state and non-market interests is the Noncommercial Stakeholder Group (NCSG) of the Generic Names Supporting Organization (GNSO).

The GNSO, which develops policy recommendations for generic top-level domains, is sub-divided into four broad stakeholder groups for policy development through working groups of interested participants. Besides the NCSG, the four broad stakeholder groups in the GNSO include the Commercial Stakeholder Group (CSG), the Registrars Stakeholder Group, and the Registries Stakeholder Group. Since the other three stakeholder groups all represent various business interests, the NCSG is the only place in the GNSO specifically reserved for non-business interests. The CSG houses three constituencies of specific business interests including the Intellectual Property Constituency, the Business Constituency, and the Internet Service Providers Constituency. The three commercial constituencies have been historically dominated by a small handful of large trademark interests who vote as a block on policy issues.

The constituency within the NCSG that promotes non-commercial interests in policy development is the Noncommercial Users Constituency (NCUC). The NCUC represents more than 600 non-profit organisations and individuals who wish to advance non-commercial policy objectives at ICANN such as human rights, education, access to knowledge, freedom of expression, privacy rights and other non-commercial goals. The NCUC's members include universities, civil liberties groups, free software groups, religious organisations, artistic groups, ICT development organisations and other non-commercial actors dedicated to the public interest.