Statement of the Noncommercial Stakeholders Group on the 8 March 2018 Model for GDPR Compliance

11 March 2018

The Noncommercial Stakeholders Group (NCSG) appreciates this opportunity to comment on the proposed interim compliance model that was published on 8 March 2018, to accommodate WHOIS in a post-GDPR landscape. While the model is a major improvement on the current open WHOIS, it remains an inadequate solution and we would like to share our preliminary concerns with the model. Since this is the first chance to see a full analysis of the reasoning behind the model, we will doubtless have further comments after discussion within our Stakeholder Group of the analysis in this document.

Natural Person vs Legal Person

The analysis on this particular issue trails off rather inconclusively. The conclusion to not attempt to distinguish between the two at the time of registration is sound, even if only taken due to cost implications. How many criminals actually register as companies with accurate data? Once again we stress, consumers should not be encouraged to try to decipher who is behind a product or service based on the DNS. Governments should spend their time regulating e-commerce in their jurisdictions, to insist on having contact data on the website itself, if they believe that is desirable. They should also educate consumers on who to trust on the web, and what kind of security features they need to look for.

Thick WHOIS

We believe that maintaining the current thick WHOIS policy is unnecessary and requires too much data, and thus is likely to violate many data protection laws. ICANN has not minimized data collection in the recent model and a core tenet of the GDPR is that appropriate measures – one of which is data minimization – must be in place. For Europeans to have their data sent to the big US registries seems to be a violation of the Transborder Dataflow provisions of the GDPR, particularly given that the adequacy of the US replacement regime for Safe Harbor, the Privacy Shield system, is in national European courts at the moment. ICANN's waiver process has to this date not served registrars well; we would appreciate further discussion on how you plan to expedite this process.

Tiered Access Models

We believe in tiered access, however we have no confidence that the Government Advisory Committee (GAC) will be able to come up with a tiered access model that has

the required rigour and supports search for specific, authorized investigations, in the time available. This is a very difficult task. While we are in favour of tiered access, we believe the mechanism has to be developed by the community, and it should be based on established standards. You mention that it will be developed in full transparency, but that is not the same as full participation. We are a vital part of the multi-stakeholder process, because we protect the interest of noncommercial uses and users of the DNS. The GAC has demonstrated time and time again a preference for representing the criminal justice system and law enforcement agencies. We recognize the argument, of course, that citizens need protection from criminal behaviour too, but citizen rights are very often in tension with the criminal justice system.

The GAC can take on the role of identifying legitimate law enforcement agencies and developing single point of contact approaches for those law enforcement agencies. However, we do not believe they are sufficiently versed in community needs to develop accreditation standards for other organizations. The GAC has frequently complained about the speed of policy development in the GNSO because they have difficulty devoting the time to follow the activities of the Policy Development Process Working Groups; we cannot imagine how it could cope with the difficult task of determining who should get access, and for what data. If the notion is to hand the whole process development over to law enforcement via the GAC's Public Safety Working Group, we strongly object. The GAC's Public Safety Working Group has not included data protection authorities or experts among its members. It operates in secret. Given the constant tension that exists between law enforcement agencies and human rights advocates, including government-appointed officials tasked with the responsibility to protect citizens' rights, such as data protection authorities and the judiciary, it is completely unacceptable to rely on the GAC or the Public Safety Working Group to do this task.

While we wait for a proper multistakeholder process to emerge and start work on tiered access, we need to go back to Model 3 in your previous proposals. Contracted parties cannot be put at risk by forcing them to provide unaccountable access to personal data.

We would also like to note our objection to the so-called "layered access" approach, if, (as we hear it is being interpreted at the moment), that means that once an organization or individual is accredited, they get access to all data elements within a certain layer of data. This is not compliant with data protection law.

For the past 20 years the GAC has done very little to cultivate privacy protection, nor has it established a data protection authority working group. The GAC has been active in defending intellectual property rights at the cost of registrants' rights, but has not made any move in favour of WHOIS privacy. At the present time it does not appear to have the relevant expertise to do so, setting aside the Council of Europe who have observer status, and the potential for data protection experts from the European Commission to participate. Visits from privacy experts and data protection authorities have been organized by our own stakeholder group, the NCSG, or as recently happened in Copenhagen (March 2017) by the Council of Europe Data Protection Directorate. For

these reasons, we respectfully suggest that the scope of their activity in the tiered access be limited to the identification of law enforcement agencies, where they certainly have the expertise.

Once this access regime is figured out, it will be important that law enforcement agencies who are accredited to access data do not use it to stifle human rights, particularly freedom of expression and political assembly. These are difficult discussions that have taken place over many years at such fora as the Council of Europe's Cybercrime (Budapest) Convention working group, and we would be remiss if ICANN set up a system that bypassed the national due process standards each country follows. We understand the problems with the current Mutual Legal Assistance Treaty process, but those problems reflect the reality of due diligence. ICANN should not stand in as a workaround for these intractable discussions.

GDPR vs Global Data Protection Laws

While we understand that this effort is about GDPR compliance, we are disappointed that ICANN would lose an opportunity to insist on compliance with *all* data protection laws, rather than only make it mandatory to avoid violating laws where they have a stake (a potential fine of 4% of global annual revenue) in ensuring compliance. This is a very bad risk decision and shows a cynical disrespect for adherence to law.

For the past 20 years, registrars and registries have been at liberty to disregard data protection law; there are few requirements in the GDPR that are new other than enforcement. It would be refreshing if ICANN would admit this, and push contracted parties to comply with all law, not just the ones where you anticipate financial consequences for non-compliance. This kind of approach only encourages frustrated civil society actors to seek innovative ways to sue under the new Regulation. As has been well described by the parties who signed on to the ECO submission, it is extremely difficult to determine when data will be within the European Economic Area ambit. This is precisely why the new regulation takes a more explicit approach to extra-territorial reach, it recognizes the complexity of the current global Internet environment, across a wide range of factors.

Anonymous Email Mechanisms

We believe that anonymous email mechanisms as described, and captcha-enabled mechanisms will go a long way to reducing spam and harassment that end-users face. We support efforts to develop these further. In particular, this mechanism can be used to constrain full access in a tiered system. Access rights could be granted within a tier, but captcha and anonymous emails could remain in that tier to reduce data to what is necessary (data minimization) and targeted (for specific investigations).

Purpose of Processing

We appreciate the attempt to analyse the purpose of processing. Given that this model has appeared only on 8 March, when our delegation was traveling to the ICANN meeting in Puerto Rico that began on 10 March, we have not had sufficient time to provide our legal analysis of the purposes of processing. As we and our members have commented before, there is much conflation going on at ICANN over the actual purpose of processing, both in the Registration Directory Service Policy Development Process Working Group working on the new policy, and in the GDPR discussions. Briefly, we would like to make the following points:

- Use cases should not be confused with purposes in performing data protection analysis. This is particularly true when use cases have proliferated over the past 20 years based on the ability to get data freely that should have been protected under data protection law.

- The attempt to make serving the "global public interest" a legal basis for processing is fundamentally flawed, particularly when processing means providing full access to personal data for stakeholders who have assembled at ICANN but whose core activities are not fundamental to the DNS. Value added service providers, intellectual property lawyers, and domain name marketers may have considerable financial interests in getting easy access to data, but that does not mean that ICANN should facilitate that, nor that these uses of registrant data are in the public interest nor vital to the stability and security of the DNS.

- In all of the examination of registrant data and WHOIS policy (or lack thereof) that has gone on for the past 20 years, there has been an absence of focus on the fundamental criteria for selection of policy goals and requirements. There is no policy, there is only contract (the RAA), and a procedure for allowing contracted parties to comply with law. As we have said for twenty years, however difficult this discussion may be, the first thing to agree upon is the criteria on which ICANN is basing its decisions. Your model and analysis does not reflect attention to this key issue. Sadly, once again, the Registration Directory Service Policy Development Process Working Group is examining use cases, and the fighting over first principles continues to block progress in a somewhat attenuated fashion. Either compliance with law is important, or it is not. (It goes without saying that it is the position of the NCSG that ICANN must comply with the law.) If we are protecting "consumers" exactly what criteria are we using to do this? Unfortunately, because the SWAT team that was assembled in the summer of 2017 to develop GDPR compliance models started with the assembling of user stories, we are doing the same thing again. This is silly, and in our view unprofessional.

- Ensuring technical stability is about the only criterion that the ICANN community appears to agree on, and we have the SSAC to thank for bringing us back to the reality of ICANN's core mission on a regular basis (SSAC 55, 51). Please address this fundamental question lest we waste a few more years arguing about worst case scenarios.

- In this examination of purposes, it is appropriate to demand facts. ICANN has not done much research on the actual needs of domain name registrants. Most of the research done at ICANN has been to accommodate the complaints of law enforcement (e.g. see the selection of research topics which resulted from the output of the second task force on WHOIS). Before taking on board all third party representations of their needs for registrant data, there should be fact checking. We submit that there is an acute absence of that data, and this model rests on a supposition of good faith that may be shaky.

Protection of Human Rights

There has been a great deal of citation of ICANN's bylaws to support law enforcement and the security and stability of the Internet during both the GDPR and the RDS PDP discussions. We have a new Bylaw that includes respect for human rights, and its implementation in a framework. This is a perfect opportunity to apply a human rights impact assessment to this model. When we do this, we find immediately that the protection of privacy must be available to all participants in the ICANN ecosystem, not just those whose governments have passed data protection law.

Conclusion

In summary, we ask of ICANN the following:

- It is critical that the entire system of WHOIS – if it should exist at all – is redesigned to protect domain name registrants. The privacy and protection of registrants, the customers who fund ICANN's activities, must be of primary importance.

- ICANN has a duty of care to protect its registrants and not to expose those who register domain names to abuse on the basis of their personal, political, religious, ethnic, racial, and/or robust and challenging speech. This is not a GDPR concern, it is a fiduciary responsibility and one that appears in a human rights impact assessment.

- Ensure that information collected from registrants is proportionate and necessary to fulfilling ICANN's mission – and not seeking to make the lives of bullies, content police, and law enforcement easier;

- The NCSG would support a tiered access tool being developed in a true, cross-community approach, but we oppose any and all attempts to permit the GAC to come up with a tiered access 'solution' before we are provided with the opportunity to provide meaningful input. Do not sacrifice the bottom-up multistakeholder model in the pursuit of a quick solution; and

- Registrants are not 'guilty until proven innocent' and deserve due process. After all, the unbounded uses to which registrants have put domain names has changed the face of the world, the leadership of countries, and expanded the freedoms of millions.

Thank you for your consideration.

Dr. Farzaneh Badiei
Chair
Noncommercial Stakeholders Group