NCSG comments on the WHOIS conflicts consultation
https://www.icann.org/public-comments/whois-conflicts-procedure-2014-05-22-en

The Noncommercial Stakeholders Group represents noncommercial organizations and individual noncommercial users in their work in the policy and proceedings of ICANN and the GNSO. We are happy to offer these comments to the WHOIS conflicts procedure consultation.

We respectfully submit as an opening premise that every legal business has the right and obligation to operate within the bounds and limits of its national laws and regulations. No legal business establishes itself to violate the law; to do so is an invitation to civil and criminal penalties, in addition to reputational damage and a loss of the trust of their customers and business partners. ICANN Registries and Registrars are no different – they want and need to abide by their local laws.

To that end, Registries and Registrars strive to comply with their national and local laws. To do otherwise is to violate the purpose of a legal regime, to threaten the well being of the company, and to expose Directors, Officers and Employees to fines, jail, or civil litigation. In the matter of protection of personal and confidential information, which is a very newsworthy issue in the 21st century, privacy practices are a key issue in establishing consumer trust, and therefore high risk for those operating an Internet business. Even if customers have obediently complied with demands for excessive collection and disclosure of personal information up to this point, in the current news furor over Snowden and the cooperation of business with national governments engaged in surveillance, this could change with the next news story. The Internet facilitates successful privacy campaigns.

It is therefore wise and timely for ICANN to raise the questions of this proceeding, *Review of the ICANN Procedure for Handling WHOIS Conflicts with Privacy Law* (albeit at a busy time for the Community and at the height of summer; we expect to see more interest in this issue and recommend that ICANN not construe the small number of comments received to date as a reflection of lack of interest). We submit these comments in response to the issues raised and the questions asked. We would urge ICANN to consider a much broader consultation on the entire matter of what its privacy policy is; this is a tweak on a contract that contains many policy decisions regarding the collection, use, and disclosure of personal information that could benefit from a much broader public discussion. We are in a global environment, Internet users care about privacy, and companies are increasingly sharing this concern.

I Background

The *ICANN Procedure for Handling Whois Conflicts with Privacy Law* was adopted in 2006 after years of debate on Whois issues. This Consensus Procedure was the first step of recognition that data protection laws and privacy law DO apply to the personal and sensitive data being collected by Registries and Registrars for the Whois database.

But for those of us in the Noncommercial Users Constituency (now part of the Noncommercial Stakeholders Group/NCSG) who helped debate, draft and adopt this Consensus Procedure in the mid-2000s, we were always concerned that the ICANN Community did not do more. At the time, several Whois Task Forces were at work with multiple proposals which include important and pro-active suggestions to allow Registrars and Registries to come into compliance with their national and local data protection and privacy laws.

We never expected this Consensus Procedure to be an end itself – but rather the first of many steps. We are glad the discussion is now reopened and we support empowering Registrars and Registries to be in full compliance with their national and local data protection, consumer protection and privacy laws – from the moment they enter into their contracts with ICANN.

We note there have been a number of recent decisions in higher courts in various jurisdictions which impact the constitutional rights of citizens to be free from warrantless disclosure and retention of their personal information for law enforcement purposes. This reflects the time it takes for data protection issues to wend their way to the high courts for a ruling. We would urge ICANN, who otherwise sit on the cutting edge of Internet technical issues, to reflect on their role as a key global player in Internet governance. Do we lead or do we wait until we are dragged into Court, to realize our responsibilities to protect the fundamental rights of the citizens who depend on the Internet to participate in modern society?

In addition, the United Nations High Commissioner for Human Rights has recently completed an investigation into the right to privacy in the digital age.[1] The High Commissioner's report will be considered at the upcoming Human Rights Council in September 2014, including recommendations that relate to the roles and responsibilities of the private sector. For example, the report states:[2]

[1] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf
[2] Ibid, para 44.

> Enterprises that provide content or Internet services, or supply the technology and equipment that make digital communications possible, for example, should adopt an explicit policy statement outlining their commitment to respect human rights throughout the company's activities. They should also have in place appropriate due diligence policies to identify, assess, prevent and mitigate any adverse impact. Companies should assess whether and how their terms of service, or their policies for gathering and sharing customer data, may result in an adverse impact on the human rights of their users.

There are significant implications from this report which will directly impact on the national and local laws under which ICANN accredited Registries and Registrars will operate. These recommendations reinforce our call for ICANN to take a first principles look at privacy policy and ensure that data protection policies and processes are modern and human rights compliant.

II. Data Protection and Privacy Laws – A Quick Overview of the Issues surrounding the Protection of the Personal and Sensitive Data of Individuals and Organizations/Small Businesses

It is important to stress that while the discourse about data protection requirements at ICANN has tended to focus on the European Union and its Data Commissioners, as represented in the Article 29 Working Party on Data Protection, there are a great many countries which have data protection law in place, including Canada, Mexico, much of South America, Korea, Japan, Australia, New Zealand, Singapore, South Africa, and many others. It is therefore quite puzzling that ICANN does not assemble a working group to study the matter and develop a harmonized approach to the issue, rather than take this rather odd approach of forcing registrars and registries to break national and local law or seek cumbersome exemptions from the provisions of their contract.

It is also important to note that there are many levels of data protection law, from local municipal law to state and national law. There is also sectoral law which applies to certain sectors. It would be a reasonable approach to develop a policy that reflects harmonized best practice, and abide by the policy rather than engage in this adversarial approach to local law. Data protection law is overwhelmingly complaints based, so it is inherently difficult for registrars and registries to get a ruling from data protection commissioners absent a complaint and a set of facts.

In this regard, we also find it puzzling that despite the fact that the Article 29

Working Party wrote to ICANN senior management to indicate that they have reviewed the matter and reached an opinion that the practices involving WHOIS do indeed violate EU law, ICANN has not taken that message and developed a policy that guides their data protection practices, starting with a clear statement of limited purpose for the collection, use, and disclosure of personal information.

The NCSG held a privacy meeting at the London ICANN 50 meeting, which was quite well attended. While we did not specifically address or attempt to brainstorm this particular problem, we feel it is safe to summarize the following points:

- There is considerable interest, not just in civil society but in other stakeholder groups and the public, in the protection of personal information at ICANN.
- Policies and procedures such as were developed for the 2013 RAA are very puzzling to those who are engaged in government and business in the privacy field. This is not 1995, when the EU Directive on data protection was passed and was still controversial. ICANN needs to catch up with global business practice, preferably by developing binding corporate rules which would take a harmonized approach to the differing local laws. It is not appropriate for all data protection to fall away in jurisdictions where there is not yet a data protection law that applies to the provision of internet services, including domain name registration.
- NCSG is ramping up a team of volunteers to provide more detailed expertise and input on a number of privacy and free speech issues. While civil society is inherently stretched and short of resources, this is an issue that they care deeply about, and our outreach has begun to bear fruit in engaging others who are outside the immediate sphere of ICANN membership. This is important as they are part of the constituency we seek to represent.

ICANN spends considerable time on technical parameters, data accuracy, and retention. More time needs to be spent on data protection policy. In this respect, more expertise would be required as there is very little evidence of privacy expertise in the ICANN community.

Finally, we would note that this process of applying for waivers is inherently flawed. A Registrar who has not experienced a privacy complaint, or is unaware of their data protection commissioner's views on ICANN issues, is unlikely to want to approach the regulator, explain the arcane nature of ICANN business,

and ask for an opinion on whether the ICANN requirements are legal or not. This is akin to waving down a policeman while driving, and asking whether they think you are driving recklessly. Absent a clear privacy policy that sets out the purpose of collection, use, disclosure and escrow, ICANN's contractees are hardly equipped to even discuss the issue. We urge ICANN to reconsider the entire matter at a more fundamental level. We would also note that if the comments on this issue are few, it could be that registrars are keeping their heads down, a sensible position to take given the analogy cited above. This hardly furthers ICANN's goals to conduct itself in accordance with the affirmation of commitments, which does require ICANN to act in the public interest, and promote consumer trust. In this respect, the question of what that means with respect to data protection needs to be asked first.

III. Questions asked of the Community in this Proceeding

The ICANN Review Paper raised a number of excellent questions. In keeping with the requirements of a Reply Period, these NCSG comments will address both our comments and those comments we particularly support in this proceeding.
However we would first like to note that the paper appears to start from the position that the procedures involved in this waiver process simply need to be tweaked. Operating under the first principle that all business must comply with local law, there is a need for ICANN to embrace data protection law as a well-recognized branch of law which codifies well recognized business best practices with respect to the confidentiality of customer data. We submit that, if ICANN had a professional privacy officer, it is highly unlikely that he/she would recommend to senior management that the current approach be entertained in 2014.

1.1 Is it impractical for ICANN to require that a contracted party already has litigation or a government proceeding initiated against it prior to being able to invoke the Whois Procedure?

1.1 Response: Yes, it is completely impractical (and ill-advised) to force a company to violate a national law as a condition of complying with their contract. Every lawyer advises businesses to comply with the laws and regulations of their field. To do otherwise is to face fines, penalties, loss of the business, even jail for officers and directors. Legal business strives to be law-abiding; no officer or director wants to go to jail for her company's violations. It is the essence of an attorney's advice to his/her clients to fully comply with the laws and operate clearly within the clear boundaries and limits of laws and regulations, both national, by province or state and local.

In these Reply Comments, we support and encourage ICANN to adopt policies consistent with the initial comments submitted by the European Commission:

> that the Whois Procedure be changed from requiring specific prosecutorial action instead to allowing "demonstrating evidence of a potential conflict widely and e.g. accepting information on the legislation imposing requirements that the contractual requirements would breach as sufficient evidence." (European Commission comments)

We also agree with Blacknight:

> "It's completely illogical for ICANN to require that a contracting party already has litigation before they can use a process. We would have loved to use a procedure or process to get exemptions, but expecting us to already be litigating before we can do so is, for lack of a better word, nuts." (Blacknight comments in this proceeding).

1.1a How can the triggering event be meaningfully defined?

This is an important question. Rephrased, we might ask together – what must a Registry or Registrar show ICANN in support of its claim that certain provisions involving Whois data violate provisions of national data protection and privacy laws?

NCSG submits that there are at least four "triggering events" that ICANN should recognize:

> Evidence from a competent Data Protection Commissioner or his/her office (or from an internationally recognized body of Data Protection Commissioners in a given region of the world, such as the Article 29 Working Party, that coordinates interpretation of the relevant data protection and privacy laws) that ICANN's contractual obligations for Registry and/or Registrar contracts violate the data protection laws of their country or their group of countries;
>
> Evidence of legal and/or jurisdictional conflict arising from analysis performed by ICANN's legal department or by national legal experts hired by ICANN to evaluate the Whois requirements of the ICANN contracts for compliance and conflicts with national data protection laws and cross-border transfer limits) (similar to the process we understand

was undertaken for the data retention issue);

Receipt of a written legal opinion from a nationally recognized law firm or qualified legal practitioner in the applicable jurisdiction that states that the collection, retention and/or transfer of certain Whois data elements as required by Registrar or Registry Agreements is "reasonably likely to violate the applicable law" of the Registry or Registrar (per the process allowed in RAA Data Retention Specification); or

An official opinion of any other governmental body of competent jurisdiction providing that compliance with the data protection requirements of the Registry/Registrar contracts violates applicable national law (although such pro-active opinions may not be the practice of the Data Protection Commissioner's office).

The above list draws from the comments of the European Commission, Data Retention Specification of the 2013 Registrar Accreditation Agreement, and sound compliance and business practices for the ICANN General Counsel's office.

We further agree with Blacknight that the requirements for triggering any review and consideration by ICANN be: simple and straightforward, quick and easy to access.

1.3 Are there any components of the triggering event/notification portion of the RAA's Data Retention waiver process that should be considered as optional for incorporation into a modified Whois Procedure?

1.3 Response: Absolutely, the full list in 1.1a above, together with other constructive contributions in the Comments and Reply Comments of this proceeding, should be thoroughly considered for incorporation into a modified Whois Procedure, or simply written into the contracts of the Registries and Registrars contractual language, or a new Annex or Specification.

We submit that the obligation of Registries and Registrars to comply with their national laws is a matter of law and compliance. In this case, we wholeheartedly embrace the concept of building a process together that will allow exceptions for data protection and privacy laws to be adopted quickly and easily.

1.4 Should parties be permitted to invoke the Whois Procedure before contracting with ICANN as a registrar or registry?

1.4 Response: Of course, Registries and Registrars should be allowed to invoke the Whois Procedure, or other appropriate annexes and specifications that may be added into Registry and Registrar contracts with ICANN. As discussed above, the right of a legal company to enter into a legal contract is the most basic of expectations under law.

2.1 Are there other relevant parties who should be included in this step?

2.1 Response: We agree with the EC that ICANN should be working as closely with National Data Protection Authorities as they will allow. In light of the overflow of work into these national commissions, and the availability of national experts at law firms, ICANN should also turn to the advice of private experts, such as legal experts who specialize in national data protection laws. The experts' opinions on these matters would help to guide ICANN's knowledge and evaluation of this important issue.

3.1 How is an agreement reached and published?

3.1 Response. It really should not be a choice for others to make, whether you comply with your national data protection and privacy laws. That said, the process of refining the Consensus Procedure, and adopting new policies and procedures, or simply putting new contract provisions, annexes or specifications into the Registry and Registrar contracts SHOULD be subject to community discussion, notification and review. Once the new process is agreed, however, we think the new changes, variations, modifications or exceptions of Individual Registries and Registrars need not go through a public review and process. The results, however, should be published for Community notification and review, and if the request is denied, we are wondering if some kind of appeal with comment period might be useful in those instances. We would underscore how complex and potentially difficult this work-around becomes, and draw attention to our remarks in sections I & II regarding, essentially, a de novo approach to the issue.

We note that in conducting the discussion with the Community on the overall or general procedure, policy or contractual changes, ICANN should be assertive in its outreach to the Data Protection Commissioners. Individually and through their organizations, and the legally mandated Article 29 Committee in the case of the EU, they have offered to help ICANN evaluate this issue numerous times. The Whois Review Team noted the inability of many external bodies to monitor ICANN regularly, but the need for outreach to them by ICANN staff nonetheless:

Recommendation 3: Outreach
ICANN should ensure that WHOIS policy issues are accompanied by cross-community outreach, including outreach to the communities outside of ICANN with a specific interest in the issues, and an ongoing program for consumer awareness. (Whois Review Team Final Report)

This is a critical policy item for such outreach and input. This matter directly concerns the personal information of individuals, organizations and small and large businesses.

3.2 If there is an agreed outcome among the relevant parties, should the Board be involved in this procedure?

3.2 Response: Clearly, in the changing of the procedure, or the adoption of a new policy or new contractual language for Registries and Registrars, Board oversight and review is required. Once the new procedure, policy or contractual language is in place, then subsequent individual changes, variations, modifications or exceptions should be handled through the process and ICANN Staff – as the Data Retention Process is handled today.

4.1 Would it be fruitful to incorporate public comment in each of the resolution scenarios?

4.1 Response: We think this question means whether there should be public input on each and every exception. We respectfully submit that the answer is No. Once the new policy, procedure or contractual language is adopted, then the process should kick in and the Registrar/Registry should be allowed to apply for the waiver, modification or revision consistent with its data protection and privacy laws. Of course, once the waiver or modification is granted, the decision should be matter of public record so that other Registries and Registrars in the jurisdiction know and so that the ICANN Community as a whole can monitor this process' implementation and compliance.

Step Five: Public notice

5.2 Is the exemption or modification termed to the length of the agreement? Or is it indefinite as long as the contracted party is located in the jurisdiction in question, or so long as the applicable law is in

force?

5.2 Response: We agree with the European Commission in its response,

> "*By logic the exemption or modification shall be in place as long as the party is subject to the jurisdiction in conflict with ICANN rules. If the applicable law was to change, or the contracted party moved to a different jurisdiction, the conditions should be reviewed to assess if the exemption is still justified."*

Provided it is the same parties, operating under the same laws, the modification or change should continue through the duration of the relationship between the Registry/Registrar and ICANN.

5.3 Should an exemption or modification based on the same laws and facts then be granted to other affected contracted parties in the same jurisdiction without invoking the Whois Procedure?

5.3 Response. The European Commission in its comments wrote, and we strongly agree: *"the same exception should apply to others in the same jurisdiction who can demonstrate that they are in the same situation."* Further, Blacknight wrote and we support: *"if ANY registrar in Germany, for example, is granted a waiver based on German law, then ALL registrars based in Germany should receive the same treatment."* Once a national data protection or privacy law is interpreted as requiring and exemption or modification, it should be available to all Registries/Registrars in that jurisdiction.

Further, we recommend that ICANN should be required to notify each gTLD Registry and Registrar in the same jurisdiction as that of the decision so they will have notice of the change.

We thank ICANN staff for holding this comment period.

Respectfully submitted,
Rafik Dammak
Chair, NCSG
On behalf of the Noncommercial Stakeholders Group

R. Dammak