Comments of the Non-commercial Stakeholders Group

GNSO Privacy & Proxy Service Accreditation Issues WG Initial Report

Due: 7 Jul 2015 23:59 UTC

Overview: Privacy/Proxy Services enable the fundamental human right of communicating speech, expression, dissent and political contributions by providing a means to avoid disclosure of one's name and address on the communications. Releasing the name of the individual or group might expose them to a range of abuse, from ridicule to death threats and actual harm.

We know that people use domain names to share the widest variety of speech and expression ever seen in the history of the world. Domain names are used for listservs, email addresses and websites that present to small groups and to the world an array of speech, both popular and unpopular, that question our assumptions, biases, political views, personal views and prejudices. They also enable teaching of banned subjects, and access to knowledge, from maternal health to democracy and freedom of religion.

For those who used the Whois database in the old days, under the Arpanet and NSFnet rules, the Whois data of name, address, phone and email represented a professional person with a business address, e.g., Scott Bradner at his Harvard Information Technology Office, his office phone and his work email.

Now the Whois database includes those who would oppose a dictatorial government, condemn an abusive corporate practice, are LGBT in countries where it is illegal, shelter the abused, or seek to share their personal, social, religious and political views. For these individuals, organizations, small businesses and even large corporations, the Whois points a finger at the name, physical address, personal cell phone (often) and email of those engaging in and leading these lives, ideas, challenges and questions.

It is no wonder that when, in the early days of ICANN, committees could not increase privacy, the market did. Domains by Proxy and others offered to place their addresses, emails, phone numbers and (if a proxy service) name, for those who sought privacy protections.

And we know that privacy is legitimate - as individuals, their personal data is protected in the many regions and countries with data protection laws.

Anonymous political speech is protected under the US First Amendment and recent Supreme Court cases, and that the right to speak legally in any medium without persecution is protection by the UN Declaration of Human Rights, Article 19.

Thus, in reviewing the proposed new rules that will formalize for the first time the relationship with proxy services, we are concerned about how to protect the domain users if we require disclosure of personal, sensitive, organizational and small business data. Since there might be no judicial process or court order, we must be very careful to balance the rights of privacy that are being relinquished, the rationales, and the procedures being proposed to ensure that full protections for speech, expression and privacy are provided.

The NCSG and the individual undersigned members submit that these comments in response to the PPSAI WG's call for comments. ICANN needs to consider carefully this guidance and direction from the Community to the WG on the sensitive and far-reaching new rules now being negotiated.

1. Proxy-Privacy registration should be available to all.

NCSG agrees with the consensus view of the PPSAI WG that proxy and privacy registrations services should be available to all who seek them and use them for legal purposes. This would include noncommercial organizations, non-profit groups, individuals, home-based business owners and numerous others. There are many reasons that a registrant might be sought by a third party for nefarious purpose – including a government tracking down a dissident organization and an ex-spouse seeking the location of a woman who owns a home-based business (both actual examples) – and the WG should recommend that ICANN continue this very legitimate, indeed fundamental, protection for all Internet users.

Neither should the WG adopt or even continue debating the minority position of some corporate participants seeking to ban the use of Proxy-Privacy registration services for those engaged in commercial transactions. Such an inquiry into the use of the domain name – the content associated with the domain name's email address, listservs and websites – is far outside the scope and mission of ICANN. ICANN has no remit to inquire into what use is made of a domain, or what content is on a website, nor to compel registrars to do the same .

Such an inquiry would lead to a never-ending series of questions regarding what is commercial, what is noncommercial, what are financial transactions and what are not. If a battered women's shelter operates on a noncommercial, not-for-profit basis, but is none-the-less incorporated as a "nonstock" corporation, should its acceptance of donations on its website be considered a commercial transaction or not? If the shelter, church, or political group, sells a T-shirt or a bumper sticker, would that change this equation? Given the immense variety of national law on what constitutes commercial

activity, could one realistically ask registrars to investigate their customers and reach informed conclusions?

The fact is that corporate structures, laws and protections for commercial and noncommercial uses and transactions vary country by country and even province by province. It is for the individual country to pass laws, as Germany has done, mandating that certain types of businesses publish physical contact information on their main webpage. This is appropriate government regulation, and it is the responsibility of nations to protect their citizens. It is not within the authority or remit of ICANN to venture into this area of activity.

The debate is also complicated by the fact that the vast majority of small and home based businesses (the ostensible target of this vocal minority proposal) are using third-party payment processors (such as PayPal) and thus are not in possession of the payment processing data at all. This is an issue we strongly urge the WG to conclude its deliberations on and leave out of any further debate or discussion.

2. Customers of Proxy-Privacy Providers must have takedown as an option to most "Reveal" requests.

Domain name registrants, even political speakers guaranteed anonymous speech protections under the US First Amendment, must provide their contact data to register a domain name – including their home address and phone number. While in some countries, post office boxes and other third party mailing address services are available, in many other countries, they are not. Accordingly, the information that a political dissenter, religious minority group, ethnic, gender or racial organization might offer – to those who choose to gun down cartoonists, church attendees or school children – provide a physical address for acts of violence or hatred.

Prior to the disclosure of any personal data – prior to any Reveal not ordered by a court or judicial magistrate – we strongly support the requirement that all Proxy-Privacy Service Providers ("Providers") offer the option to Customers of *surrendering* their domain names rather than having their underlying Customer data revealed to a third party by their Providers. NCSG submits – and has for a long time - that maintaining the protection of the Customer's data should be the default in all processes defined by the new (PPSAI) policy.

NCSG strongly supports the proposed rule of the PPSAI that the Provider must reach out to the Customer to seek input on whether to "reveal" the Customer data and what dangers or risks that disclosure might impose. NCSG further support allowing Providers to deny requests when they have determined that the Customer may be placed in an at-risk situation by disclosure of their information to a third party or the request simply does not rise to the level required for disclosure.

3. Cost of Proxy/Privacy Services must remain affordable – and proposals in the PPSAI WG Interim Report that would rapidly raise those costs – and thereby make Proxy-Privacy services increasingly inaccessible and unaffordable to noncommercial organizations – must be rejected, including the two below.

A. We support most of the "Relay" proposals of the PPSAI – proposals that would pass on communications from registries and registrars (such as renewal notices) and also legal communications such as "cease and desist" letters that attorneys may choose to send. But under no circumstances should the cost of these Relay communications be passed on to the Customer, or to the P/P service provider.

In most cases, this is a non-issue: the vast majority of communications is and will continue to be electronic and the cost is negligible. But in the cases where there is difficulty in reaching a Customer via electronic relay, and the Communicator (such as an attorney) chooses alternative communication paths (in PPSAI WG parlance: "escalation in cases of non-contactability"), such fees must be borne by the Sender and not the Customer or service provider. This is the case in the "real world" where the FedEx or courier fees are paid by the sender of legal/"hardcopy" notices.

Such a result (charging the Sender) is also fair for noncommercial organizations many of whom are located in remote and rural areas, often without regular access to the internet or intermittent electrical service, and if a delivery fee (or fees) are imposed on these Customers

-- without choice, notice or option

-- for an alleged act of the Customer that may or may not be intentional or illegal

-- by a Sender who may or may not be acting in good faith

the Customer could easily wind up being badly penalized and harmed, particularly small noncommercial organizations and noncommercial organizations based in developing nations or remote areas.

B. Under no circumstances should Intellectual Property Interests, Law Enforcement or any other Requestors have unlimited appeals to third party dispute resolution providers.

Buried in these 100 pages, and almost imperceptible to the ordinary reader, exists the proposal before the PPSAI WG that would allow any intellectual property owner (and presumably any law enforcement agency or third party security firm) who is *denied their requested Reveal of personal/sensitive data to appeal to an as-yet unknown organization for an as-yet unknown review under as yet unknown criteria for an appeal.*

o Please note that no appeal is as yet being proposed by the PPSAI WG for Customers whose request Not To Reveal was not followed by their Providers, and there is as yet no sanction to Requestors who are given Customer data and then violate the terms and limitations of its use. Absent such safeguards to protect consumers, this proposal remains half-baked. Intellectual Property owners, for example, would be able to appeal each and every rejection of their request to a Provider to a third party arbitrator and bring in solely the Provider as the alternate party. This is really quite a problematic proposal for the following reasons:

– It cuts out the major party of interest (the Customer),

--It imposes significant legal costs on the Providers who will now need to hire attorneys to argue for them in the proceedings brought against them in this future arbitration forum

-- It will impose significant costs ultimately on the Customers who will need to absorb these unfair costs to Providers in their higher proxy and privacy fees.

Accordingly, we urge our fellow Stakeholder Groups to more closely examine this little-examined appellate proposal (too rapidly placed on the table) and remove it. It will be far more than an implementation detail to define this appellate procedure – but a whole new arbitration forum of its own will need to be created and a UDRP process un-discussed and un-planned by this Working Group.

All deliberation about appeal mechanisms should be set aside at this time. Any Intellectual Property owner or group that feels a Provider is routinely denying appropriate requests will have full access to the growing and increasingly responsive ICANN Compliance Team – which will be accessible to Complainers through the accreditation process now being created.

4. Differentiation of criminal and civil requests is critical and we support the differentiation being made by the PPSAI WG.

Regarding the proposals in the PPSAI WG Interim Report, Category F: We support a strong delineation between Law Enforcement (LE) requests from LE in the country of the Proxy-Privacy Provider from LE requests in other jurisdictions and other requests of private third parties.

a. To this end, we support adoption by the PPSAI WG of the clear language of the 2013 RAA re: notification of Customers of LE requests for their data:

We recommend that providers be allowed to follow the laws of their jurisdictions of incorporation with regards to notification. A number of clients commented that there is a distinction between a request not to notify and being compelled not to notify under law, this distinction should be recognized

by the working group during its deliberation on notification of requests by LEAs."

b. We further support clear differentiation of the requests of LE in the jurisdictions of the Provider and the Customer from LE in other jurisdictions.

To this end, we further support granting access only to LE of the jurisdiction of the Provider and ICANN. The PPSAI WG final recommendations must ensure that extraterritorial requests are not facilitated absent clear proof that the allegation of illegality is a) illegal in the country in which the domain name is registered and b) supported by existing evidence. Such a requirement will avoid the clear violation of Freedom of Expression where a communication, a photograph, or a quote is deemed illegal in one country, but clearly protected speech in the country of the speaker– such as a photograph of women without veils, a Falun Gong posting, a picture of a gay pride banner, or a quote from a company's literature which is "fair use" for purposes of commentary or critique.

Under no circumstances must the identity of speakers be revealed to governments or individuals if such speech is lawful protected speech under the laws of the country in which it was created and posted – absent a legitimate judicial order, which is binding on the Provider.

To do otherwise is to jeopardize the lives and well-being not only of the speaker, but of his/her/its family, compatriots, or fellow organizations in countries where their speech may be persecuted and where sanctions including prison (or worse) may be imposed.

5. An As-Yet Unevaluated Issue: Retention and security considerations of revealed data by the requesting party - Category F.

We note that two important items may not have been considered by the working group. Currently the disclosure framework does not specify the retention period of information transferred to a third party. We recommend that a specific retention period should be developed by the working group and incorporated into the disclosure framework.

We also note that for registrants who are located within the European Union (EU) the transfer of registration data between parties constitutes a transmission of personal information under the EU Data Protection Directive 95/46/EC. This being the case, for reveal requests where the address of the registrant is located within the EU, the requestor must be able to provide evidence of compliance with the directive or the relevant compliant national law, including but not limited to identification of the Data Controller and technical security safeguards for the information once received. For requestors located in the United States a Safe Harbor certificate should be given to the service provider to demonstrate compliance and facilitate any potential action taken by the end user of the domain.

We would recommend that the working group consider the mandatory use of encrypted communications channels during the transmission of all PII regardless of the jurisdiction of the registrant and requesting party as a matter of technical best practice. Adopting such a best practice to protect Internet users would demonstrate a commitment by ICANN that it operates in the global public interest.

6. Under no circumstances must Proxy/Privacy services be Banned for so-called "commercial uses" or even so-called "financial uses" - Category C.

We are very much in agreement with the majority opinion at stated in the initial report. Eligibility for P/P services must remain open to all. It would be highly inappropriate for ICANN to make a policy decision otherwise, especially because it addresses content over the Internet, and the end use of a website or domain. Additionally we note that many noncommercial registrants utilize third party services for processing noncommercial transactions. Some examples would be soliciting donations to support a cause, promoting a crowdfunding campaign with an onsite link to donate via a crowdfunding platform such as Kickstarter or IndieGoGo. The opinion was quite strongly held that raising funds in such a manner to promote noncommercial causes should under no circumstances prevent a registrant from utilizing a P/P service.

A number of noncommercial actors noted that there was a large degree of variance in local laws with some jurisdictions not offering any form of non-individual legal personhood other than a commercial company. In this situation, a limited subset of organizations working on a nonprofit and charitable basis are incorporated in this jurisdiction as a commercial entity. We do not think the minority situation should set rules for the majority, and in any case consumer protection in financial matters on the web is a policy matter for national governments to decide, not ICANN.

If the working group decides that a compromise is required in order to reach consensus, a highly granular distinction must be made in order to prevent the exclusion of registrants from utilizing P/P services who are in need of such services due to their at risk status.

We believe that adding an additional field in WHOIS to differentiate between commercial and non-commercial registrants would be overly complex and may result in unnecessary burden on both registrars and registrants, creating a chilling effect on speech

7. There should be no appeals at this time for rejection of the Reveal requests.

In the current draft, there are no thresholds, limits, tests or boundaries for appeal -- any over-zealous intellectual property owner whose request for a reveal is carefully evaluated and rejected by the Proxy/Privacy Provider will be allowed an appeal - an ex parte appeal at that, in which the

Customer/Registrant is not even notified or allowed to fully participate in the matter. This is patently unfair, in our view and violates fundamental principles of due process of law, which require fairness in such processes where people's rights are impacted

The working group has clearly not debated this proposal sufficiently, nor given adequate consideration to important legal safeguards including due process. The proposed process, as we understand it would have the following likely results:

a) a new infrastructure of "external experts," like WIPO Panelists, would be paid and overseen by ICANN,

b) The appeal process would provide incentive and opportunity for Providers to grant the Reveal Requests routinely and without close review so that they are not drawn into expensive and time-consuming appeals processes,

c) the complete loss of rights for Customers/Registrants who not only have no appeals themselves, but are cut out of the loop of an appeals negotiation as large intellectual property owners threaten Proxy/Privacy Services. Issues such as costs, liability, and threats of lawsuits will become more central to the debate than privacy, freedom of expression, and legitimate rights of Registrants.

Under no circumstances should the "unlimited right of appeal" continue to final adoption by the PPSAI as it incentivizes inadequate, but persistent complainers. This is a contractual compliance issue and if there are problems with a Provider's performance, they will now be bound to the ICANN contractual system, and ICANN's Compliance staff will be able to act on the matter swiftly. There is no need to create unnecessary extra processes and we risk great harm in doing so in this manner.

Respectfully submitted,
The Non-Commercial Stakeholders Group (NCSG)
and the following undersigned members:

###