Briefing: ICANN moves to develop accreditation requirements for Privacy Proxy Services:
Why you and your organization should care!

ICANN Privacy and Proxy Services Accreditation Issues

ICANN, is the Internet Corporation for Assigned Names and Numbers. Tasked with managing the assignment of Names and Numbers on the Internet, ICANN operates to enact its policy through contract. Registrars must be accredited to sell domain name registration services to registrants, and this is done through contract. One of the responsibilities of registrars is to collect detailed personal or sensitive contact information of registrants in order to ensure that contact information for each domain name registered, appears in the WHOIS directory. This is a public directory available globally, which is operated by the registrars.

In response to the mandatory release of their customer's confidential information, privacy proxy services have developed, whereby registrants make arrangements with PP service providers to use their information in the WHOIS, rather than that of the beneficial registrant or domain owner. This service is provided by many accredited registrars, but there are also providers who have no contracted relationship with ICANN. The recommendation was made by the WHOIS task force, that these service providers should be accredited too, in order to ensure certain standards of data accuracy and accountability are maintained. Accordingly, a working group was struck to develop policy recommendations. The first report of this working group or PDP has been published here https://www.icann.org/public-comments/ppsai-initial-2015-05-05-en , and ICANN is seeking comments on this first draft until 7th July 2015.

Civil Society Issues

The work of the Privacy/Proxy Services Accreditation Services Issues working group, hereafter referred to as the PPSAI WG, will impact all groups and individuals who value the ability to protect their private information online. Civil society has argued for greater confidentiality and privacy in the WHOIS directory over the past 15 years, as various task forces have studied the issue. However, success has been very limited, so we advise anyone who values their privacy to use proxy services. When registering a domain name one generally must submit to having their name, address and contact information displayed publically in the directory known as WHOIS. Many registrants are unaware of this, or do not pay attention to the warnings they receive at the time of registration. Few jurisdictions with privacy law are enforcing the requirement to protection personal information, and in any case this does not help organizations such as community groups, political groups, journalists or at risk organizations such as women's shelters. Many who wish to retain the privacy of their registration details, both for reasons of personal privacy, and for at risk persons and organizations who feel that they may be placed in danger by having their contact information displayed publically, therefore use Privacy and Proxy registration services.

In general, we support the effort to bring greater rigor into the process of registering using proxy services; it is a fact that some PP service providers do not respond to allegations of criminal conduct, and disappear upon investigation. It is our position however that these groups are in the minority, and pressures to hold proxy services to a higher standard of data verification will either drive the criminal element to use more identity theft for registration purposes, defeating the purpose of data verification, or will drive costs so high that service providers will no longer offer it. This process of accreditation is therefore critically important: and excessive burden on users or providers may drive the service out of existence.

Briefing: ICANN moves to develop accreditation requirements for Privacy Proxy Services:
Why you and your organization should care!

Key Risks and Provisions

- PROCESS FOR RELAYING REQUESTS: Service providers have indicated that they receive many requests to pass email or other traffic to their clients. In many cases, this is spam, and in some cases, the registrant specifically does not want to be contacted. We support leaving relay largely to the discretion of the service provider, with the exception of legally important issues which reach a certain threshold and must be relayed to the client. In the event that email has been transmitted and the client does not respond, there should be a way for the service provider to deliver postal mail, but it must be at the expense of the requestor, not the client or the service provider.

- REVEALING PRIVATE INFORMATION: The initial report of the working group has set out an example process for disclosure of private registration information based on an allegation of copyright or intellectual property infringement, and non-response from the client. The working group has not yet formulated an example process for law enforcement requests, we believe that designing this framework for LEA requests is also critically important.

- POSSIBLE COST INCREASES FOR SERVICE PROVISION: The working group has not yet decided who is to bear the cost for transmission of hard copy documents, for repeat attempts to reach the client, and for added data verification. We believe that the costs should be borne by the requestor. Any increased costs introduced by this policy should not be borne by the registrant. This is particularly important for groups who do not have regular funding sources or who exist in the developing world. We must keep the cost burden fair on all registrants.

- DIFFERENTIATING BETWEEN CIVIL AND CRIMINAL REQUESTS: We support a strong delineation between LEA requests and requests made by private third parties. Extraterritorial requests must not be facilitated by this policy, they should go through standard procedures. Requiring providers to treat LEA requests as confidential may or may not be legal in different jurisdictions, therefore it is inappropriate to expect service providers to manage such requests. We recommend that providers be allowed to follow the laws of their jurisdictions of incorporation or the law that applies to their customers, with regards to notification of a legal procedure that requires disclosure of their information.

- LIMITED SCOPE OF ICANN: It is important to remember that ICANN sets policy for the assignment of names (domain names) and numbers (IP addresses). It does not police the Internet. While it is technically possible for the ruler of the root zone to take a domain off the Internet, and certainly any Registrar has the ability to cancel a registration for just cause at any time, the practice of bringing every ill of the Internet to the door of ICANN for a remedy must, in our view, be curtailed. It is not judge and jury.

- COMMERCIAL USE OF THE DOMAIN: There is a view widely held in the intellectual property rights holder community that ICANN should limit the availability of proxy services to individuals only, that organizations are not entitled to protect their data. This has been nuanced to those engaged in commercial activity, and the working group does not agree on the definition of that. Some feel any collection of money should disqualify a group or individual, from accepting ads for micropayments, to selling a book, or advertising services for hire. There is a fundamental lack of agreement in the working group about this issue, and we regard it as a very slippery slope. In particular, anything that is left to the discretion of service providers to resolve, is likely to mean less applicants receiving the benefits of the service rather than more, since the service currently sells for around $8 annually. We are broadly in agreement with the majority opinion at stated in the initial report. 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 using PayPal or Strype, promoting a crowd funding campaign with an onsite link to donate via a crowd funding platform such as Kickstarter or IndieGoGo. We believe quite strongly that raising funds in such a manner should under no circumstances prevent a registrant from utilizing a P/P service. We also believe that this is not a matter within ICANN's remit to regulate, as it goes to the operation of websites (content) and has nothing to do with assignment of names.

Actions

We invite all interested parties to submit comments to the initial report. This is a critical moment in the future of privacy online, the authors believe that the ability to maintain a private registration should be open to all who require it. Such services protect at-risk individuals and charities around the world every day, from battered women's shelters in Ohio to human rights activists in Iran. Without your help and input the ability of many of these service providers will be at risk of being eroded. We need to demonstrate to the working group that P/P services are a key element of the internet and must be maintained as a strong and meaningful power for registrants to protect their personal information.

Comments may be filed in two ways, an online survey located at https://s.zoomerang.com/s/VTLNGF5 or by email to comments-ppsai-initial-05may15@icann.org. Please feel free to contact the authors as listed below if you require any assistance with submitting your comments.

Alternatively you or your organization may wish to endorse the Non-Commercial Stakeholders Group comments which are currently in preparation and will be posted on the NCSG website. Please contact Stephanie Perrin if you wish to endorse.

Thank you for your time,

James Gannon
Kathy Kleiman
Stephanie Perrin

The authors of this briefing paper are members of the Non-Commercial Stakeholder Group within ICANN. Kathy Kleiman (Kathy@kathykleiman.com) is a pioneering attorney, founding one of the first Internet Law practices in the United States. Stephanie Perrin (stephanie.perrin@mail.utoronto.ca) is recognized as an international expert in privacy and data protection and the social impact of technology. James Gannon (james@cyberinvasion.net) is a cyber-security and risk management expert specializing is protecting at-risks groups from online attack. The authors also submitted a minority viewpoint on the initial report located on page 96 on the initial report.