ICANN PRIVACY/PROXY SERVICES ACCREDITATION ISSUES PDP WG

COMMENTS ON INITIAL REPORT OF THE WORKING GROUP.

INTRODUCTION

Cyberinvasion Ltd is a security and risk management consultancy based in Dublin, Ireland. As part of its mission to promote a security aware culture worldwide Cyberinvasion provides pro-bono security advisory services to at risk clients around the world.

As part of our service has included advising registrants to utilize privacy and proxy registration services to protect the identity of high risk registrants, we have formulated these comments after extensive consultation with our clients. Specific consultation were undertaken with 43 individuals, 6 registered charities and 2 unincorporated associations.

Our pro-bono clients are active in the areas of Human Rights, Free Speech and peaceful social activism. Due to the nature of our relationship with our clients all responses have been aggregated and anonymized prior to inclusion in this report.

COMMENTS

Maintaining the privacy of the registrant as a default

We would strongly support requiring Providers to offer the option to surrender the domain in the case of a request for reveal of information. We believe that maintain the anonymity of the registrant should be the default in all processes defined by the policy.

We support allowing the Provider to deny requests when they have determined that the registrant may be placed in an at-risk situation by disclosure of their information to a third party.

In the situation where the provider has exhausted all means of contact without a response from the registrant we support termination/surrender of the domain to be the default action rather that proceeding with the reveal of information.

Ensuring privacy/proxy services remain affordable

Category E

The costs associated with maintaining a web presence can be a large burden to those located in the developing world. We would recommend that any additional costs beyond the fee charged by the provider to maintain the P/P service be borne by the requestor. Specifically on the issue of escalation in the case of the non-contactability by means of electronic communications, we note that many of our clients are located in remote and rural areas, often without regular access to the internet. If a fee is to be considered to contact the registrant by alternative means such as by using the postal system, this fee must not be charged to the registrant who may not have acted in bad faith, penalizing the registrant in this situation would not be acceptable and would place an unfair financial burden on registrants located in developing nations.

Retention and security considerations of revealed data by the requesting party

Category F

We note that two 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) transferal of registration data between parties constitutes a transmission of Personally Identifiable Information as per the EU Data Protection Directive 95/46/EC[1], as such 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, 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 provided to the provider to demonstrate compliance.

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.

Differentiation of criminal and civil requests

Category F

We support a strong delineation between LEA requests and requests made by private third parties. We support the use of the language from the 2013 RAA to define LEAs.

We do not support requiring providers not to disclose LEA requests not to notify registrants of a request for publication or disclosure. We recommend that providers be allows 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 requests 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.

Ensuring that extraterritorial requests are not facilitated

We further support granting access only to LE of the jurisdiction of the Provider and the 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 and Free Speech where a communication, a photograph or a quote is deemed illegal in one country, but clearly protected speech in the country of its origin – such as 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 completely legal under the laws of the country in which it was created and posted – absent judicial order 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

Granularity of 'commercial' uses

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Category C

We are broadly in agreement with the majority opinion at stated in the initial report. The legal vehicle for the registrant and its purpose should not be the driving factor in considering its eligibility for P/P services. 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 crowd funding campaign with an onsite link to donate via a crowd funding platform such as Kickstarter or IndieGoGo. The opinion was quite strongly held that raising funds in such a manner should under no circumstances prevent a registrant from utilizing a P/P service.

A small number of clients 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. As such a limited subset of organizations working on a nonprofit and charitable basis are incorporated in their jurisdiction as a commercial entity.

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.

Submitted on behalf of Cyber Invasion Ltd and 43 individuals, 6 registered charities and 2 unincorporated associations who due to the nature of their work have in the majority asked to remain anonymous.

James Gannon

Security and Privacy Practice Lead

Cyberinvasion Ltd