PPSAI – Category D - CONTACT point provided by each privacy/proxy service

Question 4 - What are the forms of alleged malicious conduct, if any, that would be covered by a designated published point of contact at an ICANN-accredited privacy/proxy service provider[1]?

Background information relevant to this question:

Information from the Whois Studies

WHOIS Proxy/Privacy Reveal & Relay Feasibility Survey Report:

- 4.2.2. Interviewee observations: Processes for responding to requests appear to be ad-hoc and performed manually on a caseby-case basis. Responders said that they automatically co-operate with local law enforcement but have trouble authenticating requests from overseas. Those initiating requests expressed dissatisfaction with providers' responsiveness. It is not clear if the reported inconsistency between those on the supply and demand side of relay and reveal requests is caused by structural problems or process/communications failures.
- 5.1.1. Recruiting Participants: Considerable effort was expended by the survey team in the last week of October to contact privacy and proxy providers. This proved to be a challenging and painstaking task. There is no central register of these providers or their contact details. ICANN staff helped locate a breakdown of providers and the number of domain names they serve.14 This list was supplemented by provider names known to the survey team and others arising from earlier research by NORC.15
  The web sites of the 50 largest providers were located and manually checked. Some sites provided no contact details at all. Others offered web forms for requesting information or technical support, usually protected by CAPTCHA mechanisms. Where these forms were available, invitations to take part in the survey were sent manually. Many of these web forms require users to choose from a predefined list of request categories—e.g., sales inquiries or technical support—that did not fit well with a notification about the survey, and it is not clear how effective that communication channel was. Further attempts were made to contact privacy and proxy providers. The WHOIS entries for their domain names were checked and email was sent to the published Technical and Administrative Contacts inviting them to participate. (Ironically, almost all of those Contacts were themselves obscured by the use of privacy and proxy services.) Many of the privacy and proxy providers identified by this outreach effort were either operated by or had close business relationships with ICANN-accredited registrars. Although all of those emails were successfully delivered, it is not known if they were read or acted upon. The feasibility survey design did not include correlation of individual outreach efforts with subsequent participation in the survey, so it is not possible to quantify the impact of those efforts on survey participation.

---

[1] The WG noted that having a published point of contact may mean it will be used for both legitimate and spurious purposes.

Information from the EWG Survey

P/P Service Contracts and Customer Support

7 providers published customer contact information on their website, but just two of those explicitly included a phone number. One said that contacts were not published because they varied by TLD and customer, while another explained, "P/P Provider contact information constantly changes and is not posted on the website for that reason."

Ten providers supplied links to their P/P service contracts1 and described customer support services:

- Privacy and Proxy are available to be purchased and applied to domain names either directly, during the normal domain order process as well as within the member's console. Once the service has been purchased and assuming it remains active the client can either active or deactivate the service at will. Customer Support can access the same via the customer management system.
- Our customer support is available by phone or by email P/P. Customers access these services like any other customer would.
- At registration, we offer our own proxy details for [redacted] ccTLDs (not gTLDs) in case the customer refuses to disclose passport numbers, VAT numbers, etc. Customer requests are processed to either register with privacy or enable privacy afterward, again using our own privacy details.
- Each of our clients has a dedicated account manager that he can call/email/contact by mail directly. When the dedicated account manager is not present, one of his colleagues will be able to respond directly to the client.
- Our clients or potential ones can also call/email/write to our commercial team. Some offers can be ordered online and some others like Proxy or Privacy can't.
- Customer service is available by phone, email, and Live Chat. Privacy customers access our Support team via those standard methods. Privacy customers can purchase the service at the same time as purchasing the domain name, or after registration they can add the service to an existing domain through their control panel.
- This control panel also allows suspension of the privacy service.
- Customer support services are accessed through [redacted]. Customers access these services by logging into their account and clicking the P/P link associated with their domain.
- We have a "contact us", "contact owner " and "report abuse" form which goes straight through to our support team, they take the appropriate action from there.
- Customer Support for [our] service is provided directly by the Sponsoring Registrar of the domain name. The ability to disable and enable privacy services is available to all Sponsoring Registrars and their customers using [our] service. Basic questions a Registrar faces is documented here: [redacted]. [This] knowledge base article is available to every customer on the Sponsoring Registrar's platform. FAQs are also documented on [our] website - http://[redacted]/faqs/
- [We] offer customers an online support community to assist with all its products, including My Private Registration. This community is available via the URL: [redacted]. Phone, email and postal mail support is also available for customers. These services are described on our

website: [redacted]

From the Whois Review Team Final Report
Recommendation 10 - Data Access -- Privacy and Proxy Services
(…) The Review Team considers that one possible approach to achieving this would be to establish, through the appropriate means, an accreditation system for all proxy/privacy service providers. As part of this process, ICANN should consider the merits (if any) of establishing or maintaining a distinction between privacy and proxy services. The goal of this process should be to provide clear, consistent and enforceable requirements for the operation of these services consistent with national laws, and to strike an appropriate balance between stakeholders with competing but legitimate interests. At a minimum, this would include privacy, data protection, law enforcement, the industry around law enforcement and the human rights community. ICANN could, for example, use a mix of incentives and graduated sanctions to encourage proxy/privacy service providers to become accredited, and to ensure that registrars do not knowingly accept registrations from unaccredited providers.

ICANN could develop a graduated and enforceable series of penalties for proxy/privacy service providers who violate the requirements, with a clear path to de-accreditation for repeat, serial or otherwise serious breaches.

In considering the process to regulate and oversee privacy/proxy service providers, consideration should be given to the following objectives:
(….)
- Providing full WHOIS contact details for the privacy/proxy service provider, which are contactable and responsive;
(…)

What are the forms of alleged malicious conduct, if any, that would be covered by a designated published point of contact at an ICANN-accredited privacy/proxy service provider?	**Who**	**WG Response/Discussion**	**Recommended Action (if any)**
Question not clear, but p/p providers should have agreements with their customers that requires compliance with the registration agreement with the registrar (which should already have standards for conduct). If breached,	Withheld	The WG noted the following suggestions made by WG survey respondents as possible starting points for developing guidelines or a	

p/p provider should cancel the registration and notify the registrar of record.		framework for "malicious conduct" per this Charter question: (1) Safeguard 2, Annex 1 of the GAC's Beijing Communique (April 2013), which states that "Registry operators will ensure that terms of use for registrants include prohibitions against the distribution of malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law. (2) Section 3 of the Public Interest Commitments (PIC) Specification in the New gTLD Registry Agreement, which provides in relevant part that: "Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision	
Don't understand the question.	Chris Pelling		
Any violation of law should suffice to represent malicious content. Important to remember that applicable jurisdiction isn't just that of the registrant or the provider, but any jurisdiction where the registrant is attempting to market goods or receive benefits.	Emily Emanuel, John Horton, and Justin Macy. Representing LegitScript		
P/p providers should be obliged to maintain dedicated points of contact for abuse; terms should be consistent with Section 3.18 of the 2013 RAA.	Keith Kupferschmid		
Contractual obligation to provide: (1) full and accurate p/p provider information in all Whois entries using a p/p service; (2) potential for revocation and liability if p/p provider does not comply with Relay & Reveal procedures.	Jim Bikoff, David Heasley, Griffin Barnett, Valeriya Sherman / Silverberg, Goldman & Bikoff, LLP		
Difficult to identify all possible forms of malicious conduct; refer to Safeguard 2 of Annex 1 in GAC advice on new gTLDs.	Gema Campillos		
Malicious conduct should include, but not be limited to, the facilitation of actions such as IP infringement, SPAM, DDoS attacks, etc.. Any domain found to facilitate illegal activity, knowingly or otherwise, should fall under the umbrella of malicious conduct. At least piracy, trademark or copyright infringement, cybersquatting, or counterfeiting should be covered (cf. PIC Specification 3 of all new gTLD registries).	IPC		

Ambiguous question; if referring to conduct on the part of the p/p provider, WG to discuss when and how provider must respond or be able to restrict inquiries, esp when coming from (a) known bad actors (e.g. people intentionally and purposely harassing an organization over its ideas, orientation or purposes; (b) frivolous actors (e.g. those known for harassing competing businesses or other groups and individuals without basis; and other reasons for rejecting or ignoring ill-intentioned, bad faith or ultra-voluminous requests or demands by third parties for p/p service provider resources.	NCSG	prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name."	

	What are the forms of alleged malicious conduct, if any, that would be covered by a designated published point of contact at an ICANN-accredited privacy/proxy service provider?
WG Preliminary Conclusion	The WG recommends standardizing reporting forms, which would nonetheless continue to include space for free form text. A starting point for such a form could be that used under the Digital Millennium Copyright Act (DMCA) in the United States. It was also suggested that providers have the ability to "categorize" reports received, in order to facilitate responsiveness.
Should the same conclusion	

apply to proxy services & privacy services? If not, please explain why.	