**Privacy & Proxy Services Accreditation Issues (PPSAI) PDP Working Group**

**Public Comment Review Tool (Part 2)**

**7 August 2015**

For background and the general public comments received, please see <http://forum.icann.org/lists/comments-ppsai-initial-05may15/>. For a summary analysis of all the template responses received, please see the WG wiki space at: <https://community.icann.org/x/KIFCAw>.

| **#** | **Recommendation / Comment** | **Additional Comments/Notes** | **Who / What** | **Suggested WG Response** | **WG Response/Action** |
| --- | --- | --- | --- | --- | --- |
| **10. Do you agree with the WG's recommendation that: (1) ICANN should publish and maintain a publicly accessible list of all accredited P/P service providers, with all appropriate contact information; (2) registrars should provide a web link to P/P services run by them or their Affiliates; and (3) P/P service providers should declare their Affiliation with a registrar (if any) as a requirement of the accreditation program? (Section 1.3.1 Recommendation 10, Section 7.1 Category D-1)** |
|  | Support |  | BC |  |  |
|  | Support |  | ICA |  |  |
|  | We do not support creating a list of accredited service providers, however a list of providers that have committed to the recommendations would be helpful.  |  | Key Systems |  |  |
|  | Yes |  | 41 template respondents |  |  |
|  | No |  | 36 template respondents |  |  |
|  | Yes to some (no additional comment to explain) |  | 1 template respondent |  |  |
|  | Yes | ICANN should publish and maintain a publicly accessible list of all UNaccredited P/P service providers who are no longer accredited and the date when they lost their accreditation. We want to know who the bad actors are too!  | John Lawrence |  |  |
|  | Yes | Accredited P/P providers should be updated at least twice annually. | Kelly Andersson |  |  |
|  | Yes | Relevant for the registrant to know beforehand which P/ P are available, their affiliation with which registrar wherever logical places registrants will look fro information - ICANN, Registrars or P/P service providers. | Vanda Scartezini |  |  |
|  | Yes - As long as it is not infringing upon personal privacy, a list of accredited PP services and affiliates seems acceptable. |  | Dan M. |  |  |
|  | Yes - plus require P/P actually respond to requests. |  | Gary Miller |  |  |
|  | Yes to some: (1) This should be at registrars' discretion(2) This should not be a requirement for accreditation  |  | Donuts |  |  |
|  | Yes to some. I believe ICANN should publish a list of P/P providers that want to be listed and adhere to the rules and guidelines established - maintenance of that list should be minimal. I don't believe it's important that P/P providers declare an affiliation as a requirement for accreditation. |  | Dr. M. Klinefelter |  |  |
|  | Yes with conditions | "Appropriate contact information" is not defined and subject to litigation. The term "appropriate" needs to be replaced with specific requirements. | Michael Ho |  |  |
|  | No | To hell with the accreditation program in its entirety, thank you very much. We don't need it; besides which it is an offense against the privacy of us, "the people". You should be moving in the opposite direction - towards lessening the amount of personal information required and collected (directly or through registrars / providers) from individual registrants / customers. | Jawala |  |  |
|  | No | No, no, no! Get out of the P/P business. I don't want accreditation. I don't even want a public WHOIS database. But even if the database isn't going anywhere, all you should be doing with P/P providers is making sure the contact information they provide is accurate. Leave the rest to the market. I see zero benefit to me as an individual to you guys meddling. | Aaron Dalton |  |  |
|  | No | This will cripple independent P/P services. It effectively extends your monopoly over domain registration. | Stephen Black Wolf |  |  |
|  | No | I believe that accreditation of these service providers is unnecessary. It may only serve to benefit special interests who are otherwise obstructed by current proxy/privacy service providers. | C. |  |  |
|  | No | There is no need to have a list of accredited and controlled list of such providers which would undermine people's privacy. Just let the existing system continue. In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered. | Anand S. |  |  |
|  | No | This assumes that all privacy or proxy service providers are advertising their services to the general public. For persons needing to contact a specific provider, the contact information is already in WHOIS. This proposal requires all providers to be listed publicly, and thus enables malicious third parties to determine conclusively whether a given site is or is not using a provider, eroding that site's security. (For example, such a third party could send false emails to the WHOIS email contact, including the provider as an intermediary if and only if the site uses a provider.) No objection if all lists and links are voluntary, since providers will then be able to decide and respond to this issue for themselves. | Jason Burns |  |  |
|  | No | Centrally located information has inherent risk for breaches and privacy violations. This would create a target rich with information for hackers. | Jason Weinberg  |  |  |
|  | No | No accreditation should be required. | Shane T. |  |  |
|  | No | It is not and should not be ICANN's responsibility to manage P/P services. If you wish to create an independent, voluntary accreditation program with clear and reasonable criteria--reasonable from a person's perspective, not a corporation's perspective--I would support that. But the system described here is dangerous and worrying. Independent P/P services are much more meaningful and valuable for privacy than anything tied to a registrar, or a single accrediting agency, could possibly be. | Finn Ellis |  |  |
|  | No | I disagree with any text relating to an accreditation program. I do not want to see an accreditation program come into existence. | Aaron Holmes |  |  |
|  | No | No to an accreditation program. A centralized accreditation process will ensure that over time privacy will be weakened. In this case specifically, it is known that the intention is to weaken privacy. | Anonymous Turtle |  |  |
|  | --  | All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it. | Ian McNeil |  |  |
|  | No to 1. Yes to 2 and 3. Providers should be accredited and their privacy/proxy affiliation disclosed. This accreditation should not be able to be contingent, however, upon the behavior of the P/P service and P/P services should not require any sort of accreditation. |  | Andrew Merenbach |  |  |
|  | Disagree with (2). There are way too many affiliates to provide links to. They change too often. It's unlikely to provide a complete or clarifying overview. |  | Arthur Zonnenberg |  |  |
|  | (1) and (2) are unnecessary; privacy/proxy services are already easy for consumers to find. I suspect that (3) happens in most cases already, but it's not a bad idea. |  | Nick O’Dell |  |  |
|  | No | They should not be regulated. | James Ford |  |  |
|  | No | ICANN should not be in the business of accrediting P/P service providers. | Not your business |  |  |
|  | No | Due process per the law of the domain owner's country should be required before revealing information. | TS |  |  |
|  | No | Hell no! The free market will handle these issues, not the unelected. | Christopher Smith |  |  |
|  | No | This is not in ICANN's domain is it? What's next, only ICANN accredited content on a site? | D. Miedema |  |  |
|  | No | ICANN should not define, track, or control privacy companies. | Private |  |  |

|  |
| --- |
| **11. Do you agree that providing a “designated” rather than a “dedicated” point of contact will be sufficient for abuse reporting purposes, since the primary concern is to have one contact point that third parties can go to and expect a response from? Do you also agree that the designated point of contact should be capable and authorized to investigate and handle abuse reports and information requests received (a standard similar to that currently required for a Transfer Emergency Action Contact under the Inter Registrar Transfer Policy)?(Section 1.3.1 Recommendations 11 & 14, Section 7.1 Category D-2)** |
|  | Support |  | BC |  |  |
|  | Support |  | ICA |  |  |
|  | Yes |  | 40 template respondents |  |  |
|  | No |  | 32 template respondents |  |  |
|  | Yes with conditions (none specified) |  | 4 template respondents |  |  |
|  | Yes | Designated versus dedicated sounds more appropriate. | Dan M. |  |  |
|  | Yes | And a time limit to respond needs to be set. | Gary Miller |  |  |
|  | Yes | We agree that a "designated" point of contact is sufficient, provided this role is not limited to a single person (but rather is one others can operationally fulfill). | Donuts |  |  |
|  | Yes with a question | How does this affect the accreditation process? I'm wary of the combined authority to "investigate and handle" ("handle" being a very vague term). Would rather see a separation of duties, possibly involving third parties. | Tim Kramer |  |  |
|  | Yes with conditions | Yes I am happy to process abuse reports (I have never received any in 15 years of domain ownership) that are received by email. If someone calls me up on the phone in the middle of the night or shows up at my doorstep they will get abuse from me. Sure if my site is hacked and re-purposed for illegal activity I want to know about it. If someone show up at or call my home when I am at work and my kid is there, well, I would be very angry. So - there is no need ever to publish addresses or phone numbers - or real names - ICANN doesn't do the latter. | Name withheld |  |  |
|  | Yes with conditions | Designated point of contact may simply be an email address monitored by the company. | James Ford |  |  |
|  | Yes with conditions | The designated point of contact should be regularly reviewed for responsiveness and lose accreditation upon demonstrated lack of responsiveness. | Kelly Andersson |  |  |
|  | Yes with conditions | It should be the sole responsibility of the service provider to maintain contactability. | C. |  |  |
|  | Yes with conditions | I find that many abuse contacts do not take abuse reports seriously at all. They never report back what happened or what action they took. | J Wilson |  |  |
|  | Yes with conditions | If the Registrar's criteria has been met, the Disclosure and/or Publication of the WHOIS data to a non-law enforcement third-party should be limited to the equivalent of a Public Records search. For example, in the United States you can search the public business records of the California Secretary of State. A search for Google Inc. discloses the entity name and mailing address. But it does not expose the private email address or phone numbers of the business owner or it's employees. In addition to the basic contact information the public business records search includes the "Agent for Service of Process" which is the legal representative of the entity. I assert the ICANN P/P Service Regulations should adopt a similar policy directing Registrar's to only disclose basic contact information and "Agent for Service of Process" contact information to non-law enforcement third-parties. | Reid Baker |  |  |
|  | Yes with conditions |  I have not reviewed the IRTP, and have no opinion on the second point. | Jason Burns |  |  |
|  | Yes with conditions | In the case of an individual, the designated contact will often be themselves. If the mail can reach them without piercing their privacy shield, it might be ok. | Anonymous Turtle |  |  |
|  | No (qualified) | For me there is no need of a "dedicated contact" to provide a good service. must be clear who is the designated contact and that such contact will be responsive in a timely manner. TEAC standard in my view is suffice to support registrants. |  |  |  |
|  | Contactability need not match exactly the requirements of 2.3 of the RAA as providers have in many cases no access to modify or change registration data or take other action regarding the domain name. There is no need to have a point of contact equivalent to the TEAC. Response times also need not be as quickly as those of the sponsoring registrar. |  | Key Systems |  |  |
|  | --  | I do not understand what the heck this recommendation even means. | Aaron Dalton |  |  |
|  | -- | Let the existing system continue. In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered. | Anand S. |  |  |
|  | -- | All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it. | Ian McNeil |  |  |
|  | No | Horrible idea all around | Stephen Black Wolf |  |  |
|  | No | Not above and beyond the normal abuse channel. There is no additional ground for it. | Arthur Zonnenberg |  |  |
|  | No | This language is unclear; recommendations 10 and 14 appear to be separated deliberately to create ambiguity; and recommendation 14 includes too much content incorporated by reference. | Michael Ho |  |  |
|  | No | To hell with the accreditation program in its entirety, thank you very much. We don't need it; besides which it is an offense against the privacy of us, "the people". You should be moving in the opposite direction - towards lessening the amount of personal information required and collected (directly or through registrars / providers) from individual registrants / customers. | Jawala |  |  |
|  | No | Do not agree with who is able to request info. | Christopher |  |  |
|  | No | Due process per the law of the domain owner's country should be required before revealing information. | TS |  |  |
|  | No | I agree that ICANN should be a designated point of contact for abuse reporting and investigation, but I do not think ICANN should have the power to dictate to registrars when and when not data should be released. | Paul Robensen |  |  |
|  | No | I believe that only the original domain registrant should be able to authorise disclosure of information and should handle abuse complaints, not a third party. | Hugo Jobling |  |  |
|  | No | The services work as they should currently. It isn't broken so changing it can only make the situation worse. | Noah Greenstein |  |  |
|  | No | A P/P service should be able to operate independently of a registrar and thus not be required to be able to take any action with respect to the domain it protects. | Finn Ellis |  |  |
|  | No | It doesn't f------g matter. You sh--heads ignore us anyway. | Robin Hood |  |  |

|  |
| --- |
| **12. Do you agree with the WG's recommendation that P/P service providers should be fully contactable, through the publication of contact details on their websites in a manner modeled after Section 2.3 of the 2013 RAA Specification on Privacy and Proxy Registrations?(Section 1.3.1 Recommendation 12, Section 7.1 Category D-3)**  |
|  | Support |  | BC |  |  |
|  | Support |  | ICA |  |  |
|  | Yes |  | 49 template respondents |  |  |
|  | No |  | 43 template respondents |  |  |
|  | Yes but in a different way from what the WG recommends (none specified) |  | 6 template respondents |  |  |
|  | Yes | This is very important as many times I have been unable to contact a domain owner because the privacy service is completely uncontactable. | Reagan Lynch |  |  |
|  | Yes but in a different way from what the WG recommends | They should be contactable, but not in a way that could facilitate harassment. | Dan M. |  |  |
|  | Yes but in a different way from what the WG recommends | By email is fine | Name withheld |  |  |
|  | Yes but in a different way from what the WG recommends | I have not read the section in question, so cannot comment on its suitability. | Hugo Jobling |  |  |
|  | No | It's up to consumers whether they want to do business with a company they have no way to communicate with. Not up to the likes of the MPAA to decide how businesses provide communication options with consumers. | Marc Schauber |  |  |
|  | No | Due process per the law of the domain owner's country should be required before revealing information. | TS |  |  |
|  | No | Hell no! The free market will handle these issues, not the unelected. | Christopher Smith |  |  |
|  | No | Everyone should be permitted to use the web anonymously, especially companies providing anonymity services. | Private |  |  |

|  |
| --- |
| **13. Do you agree that a list of the forms of malicious conduct to be covered by a privacy/proxy service provider's designated published point of contact should be included? Do you also agree that these requirements should allow for enough flexibility to accommodate new types of malicious conduct, and that Section 3 of the Public Interest Commitments (PIC) Specification in the New gTLD Registry Agreement or Safeguard 2, Annex 1, of the GAC’s Beijing Communique could serve as starting points for developing such a list?(Section 1.3.1 Recommendation 13, Section 7.1 Category D-4)** |
|  | Support |  | BC |  |  |
|  | Support |  | ICA |  |  |
|  | 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. |  | NCSG |  |  |
|  | 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. |  | Cyberinvasion |  |  |
|  | Yes |  |  |  |  |
|  | No |  |  |  |  |
|  | Yes | It is clear, no need additional explanation. | Vanda Scartezini |  |  |
|  | Yes with conditions | Would recommend identifying host-country limitations as what one country considers illegal may be part of another country's charter (e.g., freedom of speech issues). In some (hopefully rare) cases, involvement the State Department (or other host country equivalent) may be required. | Tim Kramer |  |  |
|  | Yes with conditions | If you can eliminate domain name kiting and domain name speculation, please go ahead with this. | Andrew Merenbach |  |  |
|  | Yes with conditions | Malicious conduct should not be covered this way. New forms are found every day, while what may be malicious in one jurisdiction is not malicious in another jurisdiction. Compare US and EU law on privacy, for example. The US privacy law can be called malicious in our view. | Adam Creighton |  |  |
|  | Yes with conditions | ICANN should not be involved | Noah Greenstein |  |  |
|  | Yes with conditions | Safeguard 2, Annex 1, of the GAC’s Beijing Communique is a good starting point, but the list should not be flexible: there should be a specific list of narrow categories of behavior that is prohibited by registrants. The list should not expand to become a vehicle to regulate all prohibited kinds of conduct. | Nick O’Dell |  |  |
|  | Yes but disagree with using the PIC Spec or GAC advice | I agree that list of the forms of malicious conduct to be covered by a privacy/proxy service provider's point of contact should be included. I disagree that these requirements should be flexible because I believe the WG has not demonstrated historical precedent to justify that these requirements need to be flexible. I disagree with using either the PIC Specification and/or GAC Safeguard 2, Annex 1. More secure software (and anti-malware software) can protect against malware, education can help protect against phishing, etc. |  |  |  |
|  | Yes but disagree with using the PIC Spec or GAC advice | We disagree that the list of forms of malicious conduct should be limited or defined by third parties. The registry operator's acceptable use policy should be the primary authority for a P/P service provider's actions (such a list may very well be more inclusive). We agree that requirements should be flexible enough to allow additions or deletions as appropriate; we disagree with using Section 3 of the PIC specification and/or GAC Safeguard 2, Annex 1 as a starting point. | Donuts |  |  |
|  | Yes but disagree with using PIC Spec or GAC advice | There should be a documented list, but you cannot incorporate draft recommendations by reference to accomplish this. Requirements must be clear and must be specified at the time of execution of this document. It is reasonable to anticipate future forms of malicious conduct, but a blanket statement such as "any future form of malicious conduct" would outrageous, unenforceable, and a PR nightmare. | Michael Ho |  |  |
|  | No | I do not feel ICANN should not be creating or in any way participating in defining malicious conduct. This goes to ICANN policing internet behavior and that should be handled by laws and courts. | Dr. M. Klinefelter |  |  |
|  | No | Privacy providers should not be required to reveal customer identity except when legally required to do so by the law of the jurisdiction in which they operate. People should not have weaker privacy protections online than they enjoy offline. | Simon Kissane |  |  |
|  | No | Privacy providers, proxy providers, and even registrars have no business nosing about in the conduct of customers. That is (already) the responsibility of the hosting service. Do you all hope to become some new self-appointed Internet-police ? Kindly f--- off with that. | Jawala |  |  |
|  | No | Due process per the law of the domain owner's country should be required before revealing information. | TS |  |  |
|  | No | Hell no! The free market will handle these issues, not the unelected. | Christopher Smith |  |  |
|  | No | I fail to see the purpose of such a list. If you have valid contact information, that should be the extent of it. If they don't respond, you disable their domains, as you can already do. | Aaron Dalton |  |  |
|  | No | ICANN shouldn't be involved in this aspect AT ALL. | Stephen Black Wolf |  |  |
|  | No | Malicious conduct should not be covered this way. New forms are found every day, while what may be malicious in one jurisdiction is not malicious in another jurisdiction. Compare US and EU law on privacy, for example. The US privacy law can be called malicious in our view. | Arthur Zonnenberg |  |  |
|  | No | It should be the responsibility of service providers to remove illegal or otherwise malicious content hosted by their service. | C. |  |  |
|  | No | Let the existing system continue. In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered. | Anand S. |  |  |
|  | No | I object to any open-ended malicious conduct standard being imposed, since such standards are more open to abuse. If changes need to be made as technology changes, they can be adopted through the usual process. | Jason Burns |  |  |
|  | No | This should not be applicable: ICANN should not be reviewing or evaluating the content of websites, nor should it be the sole authority over people who do. | Finn Ellis |  |  |
|  | No | This sounds like b---s---. Who do you think we are | Robin Hood |  |  |
|  | -- | All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it. | Ian McNeil |  |  |

|  |
| --- |
| **15[[1]](#footnote-1). Do you agree with the WG's recommendation that a standardized form should be developed for the purpose of reporting abuse and submitting requests (including requests for Disclosure of customer information), to also include space for free form text? Do you also agree that privacy/proxy service providers should have the ability to “categorize” reports received, in order to facilitate responsiveness?(Section 1.3.1 Recommendation 15, Section 7.1 Category D-4)**  |
|  | Support |  | BC |  |  |
|  | Support |  | ICA |  |  |
|  | Yes |  | 36 template responders |  |  |
|  | No |  | 36 template responders |  |  |
|  | Yes with conditions |  | 6 template responders |  |  |
|  | Yes | A very high priority should be focused on third parties' ability to report copyright infringement, malicious or libelous content, "revenge porn" and other damaging content -- all of which should be prioritized for immediate (or very quick) takedown. | Kelly Andersson |  |  |
|  | Yes | As long as it does not facilitate harassment, again. | Dan M. |  |  |
|  | Yes | This one sounds legit. | Christopher Smith |  |  |
|  | Yes with conditions | This standard could be offered for use and P/P providers may even be required to accept them to become accredited. However, I believe the level of responsiveness is beyond the purview of ICANN. | Dr. M. Klinefelter |  |  |
|  | Yes with conditions | Disclosure should not be without the knowledge of the original registrant. | Hugo Jobling |  |  |
|  | Yes with conditions | Requests for Disclosure should be restricted to FTC, spamcop and Spamhaus unless there is a Court Order. | J Wilson |  |  |
|  | Yes with conditions | If response is not FIFO they will just ignore the reports they do not want to deal with. | Gary Miller |  |  |
|  | Yes with conditions | Templates are really a facilitator to both sides and shall be included, but not with too many specificities that will make it difficult to registrant to report . general categories plus a space to detail it would be suffice. However let me remember that languages availability is essencial. Templates shall be the same to all P/P services and shall come into at least the same languages ICANN is providing to its website. being the same document, costs to have it in the languages provided by ICANN can be diluted among P/P providers. | Vanda Scartezini |  |  |
|  | Yes with conditions | Standardised forms should allow option options for circumstances that we haven't dreamed would happen yet. I've hit form submissions where I couldn't actually submit my complaints because the form was too rigid. | Michelle Knight |  |  |
|  | Yes with conditions | Putting "conditions" in quotes, and not defining any, suggests that you don't know what they might be. By writing this recommendation in the passive voice, it seems that you are delegating this standardization to the P/P organizations. If you intend to develop this form, you must say so explicitly. | Michael Ho |  |  |
|  | Yes with conditions | Standardized forms are nice, if you must, but no category, nor any submission, should ever trigger any automated or automatic action against the customer / against the customer's services. | Jawala |  |  |
|  | Yes with conditions | It should be the sole responsibility of the service provider to handle these requests, but if a separate form is created elsewhere to make it easier for people to file abuse reports, this is acceptable. | C. |  |  |
|  | Yes with conditions | I do not believe a standard form is necessary, but one may be tried on a voluntary basis. No objection to categorizing reports. | Jason Burns |  |  |
|  | Yes with conditions | Privacy/proxy service providers should have the ability to “categorize” reports received, but should not be required to. | Adam Creighton |  |  |
|  | No | We disagree that a standardized submission form should be created; each P/P provider should be permitted the latitude to use a form suitable for their own specific services. We disagree that a freeform text option be included. We agree that P/P providers should have the ability to categorize reports if they so choose; however, they should not be required to do so. | Donuts |  |  |
|  | No | I don't think enough reports are received to warrant special categories. I have not received one report in 15 years and with about 10 domains. | Name withheld |  |  |
|  | No | Do not agree with persons able to make requests. | Christopher |  |  |
|  | No | Due process per the law of the domain owner's country should be required before revealing information. | TS |  |  |
|  | No | The only process for violating privacy should be the existing legal processes. | Private |  |  |
|  | No | Not beyond the normal abuse form already present. | Arthur Zonnenberg |  |  |
|  | No | Just let the existing system continue. In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered. | Anand S. |  |  |
|  | No | Now you’re just making s--- up. | Robin Hood |  |  |
|  | -- | All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it. | Ian McNeil |  |  |

1. In the online template of questions, Recommendations #11 & #14 were asked as two parts of a question. The numbering of the questions on this Tool has thus been changed from here, to correspond to the actual recommendations in the Initial Report. [↑](#footnote-ref-1)